IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPEAL BRIEF FOR THE APPELLANT

Ex parte HASEBE et al

STORAGE MEDIUM FOR PREVENTING AN IRREGULAR USE BY A THIRD PARTY

Serial No. 09/476,319
Appeal No.:
Group Art Unit: 2132

Enclosed is a check in the amount of Three Hundred Twenty Dollars ($320.00) to cover the official fee for this Appeal Brief. In the event that there may be any fees due with respect to the filing of this paper, please charge Deposit Account No. 50-2222.

September 30, 2003

Douglas H. Goldhush
Attorney for Appellant(s)
Reg. No. 33,125

SQUIRE, SANDERS & DEMPSEY LLP
8000 Towers Crescent Drive, 14th Floor
Tysons Corner, VA 22182-2700

Atty. Docket: 58622.09028

DHG/scc

Encls: Check No. 010528
Appeal Brief (in triplicate)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re the Appellant:

HASEBE et al

Appeal No.:

Serial Number: 09/476,319

Group Art Unit: 2132

Filed: December 30, 1999

Examiner: Gilberto Barron, Jr.

For: STORAGE MEDIUM FOR PREVENTING AN IRREGULAR USE BY A THIRD PARTY

BRIEF ON APPEAL

September 30, 2003

I. INTRODUCTION

This is an appeal from the final rejection set forth in an Official Action dated March 31, 2003, finally rejecting claims 1-56 and 111-125, all of the claims pending in this reissue patent application, as being unpatentable under 35 U.S.C. § 101. A Response under 37 CFR § 1.116 was timely filed on July 17, 2003, with an appropriate Petition for Extension of Time. An Advisory Action was issued on July 28, 2003, indicating that upon the filing of an appeal, proposed amendments contained in that response would be entered, but that the claims would remain rejected. A Notice of Appeal was timely filed on July 30, 2003. This Appeal Brief is being timely filed.

II. REAL PARTY IN INTEREST

The real party in interest in this application is Fujitsu Limited, of Kawasaki, Japan.

III. STATEMENT OF RELATED APPEALS AND INTERFERENCES

There are no known related appeals and/or interferences which will directly effect or be directly effected by or have a bearing on the Board's decision in this appeal.

IV. STATUS OF CLAIMS

Claims 1-56 and 111-125, all of the claims pending in the present reissue application are the subject of this appeal.

V. STATUS OF AMENDMENTS

Amendments were filed with applicants' Request for Reconsideration on July 17, 2003. In the Advisory Action dated July 28, 2003, box number 7 was checked, indicating that the proposed amendments will be entered, but that the claims would remain rejected. This appeal, therefore, is directed to claims 1-56 and 111-125 as presented on July 17, 2003.

VI. SUMMARY OF THE INVENTION

Since this application is a reissue application, the summary of the invention, in order to comply with 37 CFR § 1.192, will refer to column numbers and line numbers of the issued patent, United States Patent No. 5,796,824.

The claims are directed to various embodiments of a storage medium. Claim 1, as an example, is directed to a storage medium accessed by a vendor computer and a user computer, with the storage medium for storing information readable by the user

computer (see Figure 3). The storage medium includes encrypted electronic data to be decrypted by the user computer (Figure 3, item 15, and column 5, lines 20-23). A medium personal number is provided on the storage medium, with the medium personal number being particularly personal for each storage medium and is different from a medium personal number of another storage medium (Figure 3, item 12, and column 5, lines 19-26). The medium personal number is discussed as being written onto the storage medium in an un-rewritable form which the computer cannot rewrite, and the medium personal number is used for generating a decryption key for decrypting the encrypted electronic data in the user computer (see Figure 3, items 31-35, and column 5, lines 47-61). Permission information is provided which includes the decryption key encrypted in a manner that is generated independent from a specific apparatus number for a specific computer, and generated based upon the medium personal number (see Figure 3, items 31-35, and column 5, lines 32-46, and also 47-61). The permission information and the medium personal number enable the user computer to decrypt the encrypted decryption key and to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted decryption key and the encrypted electronic data (column 5, lines 47-61 et seq, and also, for example, column 10, lines 58 through column 11, line 4).

Numerous other embodiments of the invention are recited in the claims. Claim 19, as another example, is directed to a storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific first computer and which

stores the encrypted decryption key onto the storage medium, and accessible from a plurality of second computers (as discussed in column 10, and elsewhere in the present specification). Claim 19 recites various functionality of the storage medium, and indicates that the storage medium comprises a first storage area for storing encrypted electronic data to be decrypted by the second computer (see, for example, Figure 12 and column 10, lines 16-24). A second storage area is provided for storing the medium personal number, which is unrewritable from at least the second computers. The medium personal number is particularly personal for each storage medium, and is different from a medium personal number of another storage medium (see Figure 12, and also column 5, lines 23-32, and column 10, lines 16-24). A third storage area is recited for storing the encrypted decryption key, with the encrypted decryption key being generated based upon the medium personal number and the encrypted decryption key is generated independent from the specific apparatus number for the specific first computer (also, illustrated in Figure 12, and discussed at various places in column 5, and column 10 first application). Other embodiments are recited in the claims, and illustrated in the drawings, for example, in Figures 6-10, and the corresponding discussions in column 6, lines 53 through column 9, line 37 of the application.

All of the presently pending claims were finally rejected under 35 USC § 101, on the grounds that the claims are directed to non-statutory subject matter in that the claims only provide for non-functional descriptive matter. The issue in this Appeal, therefore, is whether or not claims 1-56 and 111-125 are in compliance with 35 USC § 101, and more particularly, whether or not they comply with the guidelines for computer-related

inventions as set forth in MPEP § 2106.

VII. GROUPING OF CLAIMS

Claims 1, 6, 11, 17-19, 23-29, 33-39, 43-49, 53-56, 111-113, 119, 123, 124, and 125 are all independent claims. Each of the independent claims, and the claims dependent thereupon, should be considered to be a separate group, with each independent claim therefore standing alone.

VIII. APPELLANT'S ARGUMENTS

As noted previously, the only issue in this final rejection is the fact that claims 1-56 and 111-125 are rejected under 35 USC § 101, on the grounds that the claims are directed to non-statutory subject matter. Applicants respectfully appeal from this rejection, and submit that each of claims 1-56 and 111-125 are in a form which is in compliance with United States patent practice, in compliance with 35 USC § 101, and in compliance with the guidelines regarding computer-related inventions as set forth in MPEP § 2106. It is therefore respectfully requested that this Honorable Board of Patent Appeals and Interferences reverse the Examiner's decision regarding these claims, and indicate the allowability of claims 1-56 and 111-125.

The Office Action relies heavily on the 1992 Federal Circuit decision in *Arrhythmia Research Technology Inc. v. Corazonix Corp.*, 22 USPQ 2d 1033 (Fed. Cir. 1992), as providing authority for this rejection. The Office Action takes the position that "usefulness under the patent eligibility standard requires significant functionality to be present to

satisfy the useful result aspect of the practical application requirement...Merely claiming non-functional descriptive material stored in a computer-readable medium does not make the invention eligible for patenting." (Id. at 1036). Applicants respectfully submit, however, that the *Arrhythmia* decision does not support the Office Action's position. In *Arrhythmia*, the Court held United States Patent No. 4,422,459 to be valid due to the fact that the claim at issue recited a series of steps which processed signals. Though the facts of *Arrhythmia* are not particularly applicable to the present application, the Court in *Arrhythmia* did repeatedly state that the use of mathematical formulae or relationships to describe the structure or operation of an apparatus does not make it non-statutory. MPEP § 2106 clearly states that claims which are directed to an article of manufacture is in fact statutory subject matter. The article of manufacture of all of the independent claims in the present application is a storage medium accessed by various computers or accessible by a computer. The storage medium is recited as comprising various types of data thereupon. The claims also recite a specific interrelationship between the data and the computer; for example, the presently pending claims recite that the storage medium includes either a storage area containing encrypted electronic data, or encrypted electronic data, which is to be decrypted by a computer. All of the claims recite interaction with either a first computer and a second computer, a vendor computer and a user computer, or other computers which interact and interrelate with the storage medium in the particular aspects which are recited in the claims. Applicants strongly but respectfully submit, therefore, that the reliance on *Arrhythmia* as a basis upon which to reject the presently pending claims is improper. In the Advisory Action, the Examiner

noted:

> "Applicant points out that the statement from Arrhythmia should not apply as the claims are directed to an article of manufacture. However, the claimed article of manufacture is a storage medium for storing non-functional descriptive material, which is non-statutory as there is no functionality to be imparted to a computer to produce a useful, concrete and tangible result."

Applicants submit that, based upon the statement in the Advisory Action, that the Examiner regards claimed media personal number, permission information, etc. as descriptive material as discussed in MPEP § 2106 § IV(B) (1). In this section of the MPEP, the descriptive material is discussed as music, literature, art, photographs and mere arrangements or compilations of facts or data. However, it is strongly and respectfully submitted that the various elements of the claimed invention cannot be compared to such mere arrangements or compilations of data. The claimed invention clearly defines a structural and functional interrelationship between the vendor computer and the user computer, as well as between the data and the computer.

Immediately following the description of non-functional descriptive material in the above-noted section of the MPEP, the following passage can be found:

> "Office personnel should be prudent in applying the foregoing guidance. Nonfunctional descriptive material may be claimed in combination with other functional descriptive multi-media material on a computer-readable medium to provide the necessary functional and structural interrelationship to satisfy the requirements of **35 U.S.C. 101**. The presence of the claimed nonfunctional descriptive material is not necessarily determinative of nonstatutory subject matter. For example, a computer that recognizes a particular grouping of musical notes read from memory and upon recognizing that particular sequence, causes another defined series of notes to be played, defines a functional interrelationship among that data and the computing processes performed when utilizing that data, and as such is statutory because it implements a statutory process."

The present invention can be compared to this example, in that it is directed to an article of manufacture containing elements which control the functional relationship between a vendor computer and a user computer, or a first computer and a second computer, and which results in encrypted data being decrypted by the user computer. In other words, upon recognizing certain information, another defined set of data is accessed/decrypted. This is exactly the statutory example provided by the MPEP.

Applicants note that the *Arrhythmia* case was decided on March 12, 1992; the "useful, concrete, and tangible result" standard for business method and software-type inventions was developed by the Court of Appeals for the Federal Circuit in the infamous *State Street Bank* case in 1998 (*State Street Bank v. Signature Financial Group, Inc.*, 149 F.3d 1368, 47 USPQ 2d 1596, (Fed. Cir. 1998)). Page 1036 of the *Arrhythmia* case, relied upon in the Office Action, merely contains a discussion of older and significantly modified holdings regarding computer programs and patentability which are not applicable to the case at hand. As mentioned above, the present claims are clearly directed to an article of manufacture, which is expressly indicated in 35 USC § 101 as being statutory subject matter.

Furthermore, claims 1-56 and 111-125 each recite functional relationships between the data on a storage medium and the computer, and the areas of data on the storage medium. The Office Action seems to disregard this significant issue. Though the claims are directed to a storage medium, the Office Action took the position that the claims did not recite a sufficient functional relationship between either the elements of the storage medium themselves, and/or the elements of the storage medium and the

computer. However, claims 1-56 and 111-125 each recite areas or data on a computer storage medium which imparts specific functionality to the computer, and which provides a useful, concrete, and tangible result as required by the *State Street Bank* case, the *AT&T* case (*AT&T Corp. v. Excel Communications, Inc.*, 50 USPQ 2d 1447 (Fed. Cir. 1999)), and other more recent decisions by the CAFC.

Using claim 1 as an example, the storage medium is recited as being accessed by a vendor computer and a user computer, and comprises encrypted electronic data which is to be decrypted by the user computer, and the storage medium also contains a medium personal number. The medium personal number is recited as having particular characteristics, and is used for generating a decryption key for decrypting the encrypted electronic data in the user computer. Permission information and the medium personal number enables the user computer to decrypt the encrypted decryption key and to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted decryption key and the encrypted electronic data.

The Office Action took the position that the description in the claims of a relationship between storage areas of the storage medium is an "abstract idea," and not a functional one which effects the computer or causes the computer to perform a stated functionality on any other data at a different storage area. The Office Action further cites § II of MPEP § 2106, and states that the claims, did not recite a useful, concrete, and tangible result. However, in addition to the MPEP § 2106 discussion set forth above, applicants further submit that MPEP § 2106 § IV(B)(1)(a) explains that when a computer

program and presumably a data structure is recited in conjunction with a physical structure (in this application, a storage medium and/or the user computer, second computer, etc.), Patent Office personnel should treat the claims as a product claim. Additionally, applicants respectfully submit that the MPEP clearly explains that data structures which are not claimed as embodied in computer readable media are descriptive material per se due to the fact that the claimed data structures do not define any structural and functional interrelationships between the data structure and other claimed aspects of the invention. This same section of the MPEP does clearly state:

> "In contrast, a claimed computer-readable medium encoded with a data structure defines structural and functional interrelationships between the data structure and the computer software on hardware components which permit the data structures functionality to be realized, and is thus statutory." (Emphasis added)

Therefore, applicants strongly but respectfully submit that the Office Action seems to be ignoring the fact that the claims are clearly directed to a storage medium, and are not directed to computer programs or computer listings per se. MPEP § 2106 § IV(B)(2)(a) states that "a claim limited to a machine or manufacture, which has a practical application in the technological arts, is statutory." All of claims 1-56 and 111-125 clearly recite a storage medium which is accessible by a vendor computer and a user computer, with the various areas of the storage medium or the various data on the storage medium clearly interrelating and effecting each other, and clearly interrelating with and operating in conjunction with elements of the computer. All of the claims clearly indicate that the

encrypted electronic data is to be decrypted by the user computer, and is in fact decrypted by the user computer (or the second computer, etc.), in conjunction with a medium personal number, permission information, or other information as recited in the claims. Claims 1-56 and 111-125 all recite the useful, concrete and tangible result of enabling the user computer or the second computer to decrypt the encrypted electronic data and/or the decryption key in the user computer without using a specific apparatus number for a specific computer.

The useful, concrete and tangible result which is required by *State Street Bank* is clearly provided in the recited decryption of encrypted electronic data. The current state of the law regarding computer-implemented inventions is that as long as the inventions are new, useful, and non-obvious, and provide a useful, concrete, and tangible result, the invention should be found to be statutory subject matter, and should be found to be patentable. Additionally, in other CAFC cases in the last decade, the Court repeatedly held that a transformation of data within a computer system can constitute a practical application, and therefore should be found to be statutory subject matter under 35 USC§ 101 (see, for example, *In re Allapat* 33 F.3d 1526, 31 USPQ 2d 1545 (Fed. Cir. 1994), and *Arrythmia Research* (id)). This, of course, is notwithstanding the fact that all of the claims are directed to an article of manufacture.

Applicants note that 37 CFR § 1.192 suggests that an Appeal Brief should describe the subject matter defined in each of the rejected claims. Applicants have used several of the independent rejected claims as examples of the subject matter of the invention. However, the fundamental basis for reversing the Examiner's rejection is

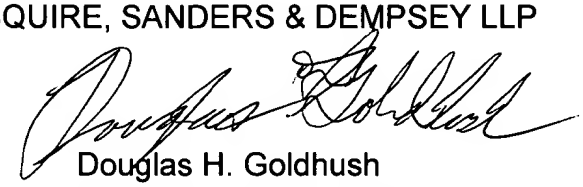
common for all of the rejected claims. That is, once again, that all of the claims are directed to an article of manufacture, which is per se statutory under 35 USC § 101. Furthermore, each of the rejected claims recite functional relationships between the data on the storage medium and the computer, and the areas of data on the storage medium and the computer. These are common to all of the rejected claims, and an individual discussion of each independent claims should therefore be unnecessary.

In view of the above, it is once again respectfully requested that this Honorable Board of Patent Appeals and Interferences reverse the outstanding rejections in this application, and indicate the allowability of all of presently pending claims 1-56 and 111-125.

In the event that this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees which may be due with respect to this paper may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

SQUIRE, SANDERS & DEMPSEY LLP



Douglas H. Goldhush
Attorney for Applicant(s)
Registration No. 33,125

Atty. Docket No.: 58622.09028

8000 Towers Crescent Drive, 14th Floor
Tysons Corner, VA 22182-2700
Tel: (703) 720-7800
Fax (703) 720-7802

DHG:scc

Encls: Appendix 1
Appendix 2

APPENDIX 1

CLAIMS ON APPEAL

1. A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

encrypted electronic data to be decrypted by the user computer;

a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which said user computer cannot rewrite, and said medium personal number is used for generating a decryption key for decrypting said encrypted electronic data in said user computer; and

permission information which includes the decryption key encrypted in a manner that is generated independent from a specific apparatus number for a specific computer, and generated based upon said medium personal number, said permission information and said medium personal number enabling the user computer to decrypt the encrypted decryption key and to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted decryption key and the encrypted electronic data.

2. A storage medium as claimed in claim 1, wherein the electronic data is software used for a computer.

3. A storage medium as claimed in claim 1, wherein the electronic data is electronically published data.

4. A storage medium as claimed in claim 1, wherein the storage medium is an optical magnetic disk, or a partially embossed optical disk.

5. A storage medium as claimed in claim 1, wherein the storage medium is a CD-ROM.

6. A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

encrypted electronic data to be decrypted by the user computer;

a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which said user computer cannot rewrite, and said medium personal number is used for generating an encrypted permission information in said vendor computer; and

permission information encrypted in a manner that is generated independent from a specific apparatus number for a specific computer and generated based upon said medium personal number, wherein the permission information and said medium personal number enabling the user computer to decrypt the encrypted permission information and to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted permission information and the encrypted electronic data.

7. A storage medium as claimed in claim 6, wherein the electronic data is software used for a computer.

8. A storage medium as claimed in claim 6, wherein the electronic data is electronically published data.

9. A storage medium as claimed in claim 6, wherein the storage medium is an optical magnetic disk or a partially embossed optical disk.

10. A storage medium as claimed in claim 6, wherein the storage medium is a CD-ROM.

11. A storage medium accessed by a vendor computer and a user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

encrypted electronic data to be decrypted by the user computer;

a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

encrypted permission information that is generated independent from a specific apparatus number for a specific computer and generated based upon said medium personal number;

wherein at least the medium personal number is written onto the storage medium in an unrewritable form which a user computer cannot rewrite, and wherein said encrypted permission information and said medium personal number enabling the user computer to decrypt the encrypted permission information and to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted permission information and the encrypted electronic data.

12. A storage medium as claimed in claim 11, wherein the electronic data is software used for a computer.

13. A storage medium as claimed in claim 11, wherein the electronic data is electronically published data.

14. A storage medium as claimed in claim 11, wherein the storage medium stores a plurality of encrypted electronic data, and each encrypted electronic data has a different electronic data decrypting key.

15. A storage medium as claimed in claim 11, wherein the storage medium is an optical magnetic disk, or a partially embossed optical disk.

16. A storage medium as claimed in claim 11, wherein the storage medium is a CD-ROM.

17. A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein the medium personal number is written onto the storage medium in an un-rewritable form which a user storage reading apparatus cannot rewrite;

encrypted electronic data to be decrypted by the user computer; and

information which is encrypted based on said medium personal number and is encrypted independent from a specific apparatus number for a specific computer and said medium personal number is used for generating a decryption key, said decryption key and said medium personal number enabling said user computer to decrypt said

encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted electronic data.

18. A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

encrypted electronic data to be decrypted by the user computer;

a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which the user storage reading apparatus cannot rewrite, and said medium personal number is used for decrypting said encrypted electronic data; and

information which is encrypted based on said medium personal number and is encrypted independent from a specific apparatus number for a specific computer, said information and said medium personal number enabling said user computer to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted electronic data.

19. A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific first computer and which stores the encrypted decryption key onto the storage medium, and accessible from a plurality of second computers which decrypt the encrypted decryption key stored on the storage medium

based upon the medium personal number and independent from a specific apparatus number for a specific second computer and which decrypt encrypted electronic data stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific second computer, the storage medium comprising:

a first storage area for storing encrypted electronic data to be decrypted by the second computer, the encrypted electronic data including electronic data encrypted based upon the decryption key;

a second storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from the specific apparatus number for the specific first computer,

wherein the encrypted decryption key in the third storage area and said medium personal number enables the second computer to decrypt the encrypted electronic data in the first storage area in a manner that the second computer does not use the specific apparatus number for the specific first computer in decrypting the encrypted electronic data.

20. The storage medium of claim 19, wherein the electronic information is software used for a computer.

21. The storage medium of claim 19, wherein the electronic information is electronically published information.

22. The storage medium of claim 19, wherein the storage medium is a read-only optical disk.

23. A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific first computer and which stores the encrypted decryption key onto the storage medium and which encrypts electronic data based upon the decryption key and which stores the encrypted electronic data onto the storage medium, and accessible from a plurality of second computers which decrypt the encrypted decryption key stored on the storage medium based upon the medium personal number and independent from a specific apparatus number for a specific second computer and which decrypt encrypted electronic data stored on the storage medium based upon the encrypted decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific second computer, the storage medium comprising:

a first storage area for storing encrypted electronic data to be decrypted by the second computer, the encrypted electronic data includes electronic data encrypted based upon the decryption key;

a second storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from the specific apparatus number for the specific first computer,

wherein the encrypted decryption key in the third storage area and said medium personal number enables the second computer to decrypt the encrypted electronic data in the first storage area in a manner that the second computer does not use the specific apparatus number for the specific first computer in decrypting the encrypted electronic data.

24. A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific computer and which stores the encrypted decryption key onto the storage medium, the storage medium comprising:

a first storage area for storing encrypted electronic data to be decrypted by a user computer, the encrypted electronic data including electronic data encrypted based upon the decryption key;

a second storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and

the encrypted decryption key is generated independent from a specific apparatus number for a specific computer,

wherein the encrypted decryption key in the third storage area and said medium personal number enables the user computer to decrypt the encrypted electronic data in the first storage area in a manner that the user computer does not use the specific apparatus number for the specific first computer in decrypting the encrypted electronic data.

25. A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific computer and which stores the encrypted decryption key onto the storage medium and which encrypts electronic data based upon the encrypted decryption key and which stores the encrypted electronic data onto the storage medium, the storage medium comprising:

a first storage area for storing encrypted electronic data to be decrypted by a user computer, the encrypted electronic data including electronic data encrypted based upon the decryption key;

a second storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and

the encrypted decryption key is generated independent from a specific apparatus number for a specific computer,

wherein the encrypted decryption key in the third storage area and said medium personal number enables the user computer to decrypt the encrypted electronic data in the first storage area in a manner that the user computer does not use the specific apparatus number for the specific first computer in decrypting the encrypted electronic data.

26. A storage medium accessible from a plurality of computers which decrypt an encrypted decryption key stored on the storage medium, the encrypted decryption key being based upon a medium personal number and independent from a specific apparatus number for a specific computer, and which decrypt encrypted electronic data stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific computer, the storage medium comprising:

a first storage area for storing encrypted electronic data to be decrypted by a user computer, the encrypted electronic data including electronic data encrypted based upon the decryption key;

a second storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing an encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and

the encrypted decryption key is generated independent from the specific apparatus number for the specific computer,

wherein the encrypted decryption key in the third storage area and said medium personal number enables the user computer to decrypt the encrypted electronic data in the first storage area in a manner that the user computer does not use the specific apparatus number for the specific first computer in decrypting the encrypted electronic data.

27. A storage medium accessible from a vendor computer and a user computer at different times, the storage medium comprising:

a first storage area for storing encrypted electronic data to be decrypted by the user computer, the encrypted electronic data including electronic data encrypted based upon a decryption key;

a second storage area for storing a medium personal number, which is un-rewritable from the computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing an encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from a specific apparatus number for a specific computer,

wherein the encrypted decryption key in the third storage area and said medium personal number enables the user computer decrypts the encrypted electronic data in the first storage area in a manner that the user computer does not use the specific

apparatus number for the specific first computer in decrypting the encrypted electronic data.

28. A storage medium accessed by a vendor computer and a user computer, said storage medium comprising:

a first storage area for storing encrypted electronic data to be decrypted by the user computer, the encrypted electronic data including electronic data encrypted based upon a decryption key;

a second storage area for storing a medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing an encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from a specific apparatus number for a specific computer,

wherein the encrypted decryption key in the third storage area and said medium personal number enables the user computer to decrypt the encrypted electronic data in the first storage area in a manner that the user computer does not use the specific apparatus number for the specific first computer in decrypting the encrypted electronic data.

29. A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific first computer and which stores the encrypted

decryption key onto the storage medium, and accessible from a plurality of second computers which decrypt the encrypted decryption key stored on the storage medium based upon the medium personal number and independent from a specific apparatus number for a specific second computer and which decrypt encrypted electronic data stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific second computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data to be decrypted by the second computer and the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from the specific apparatus number for the specific first computer, and wherein the encrypted decryption key and said medium personal number enables the second computer to decrypt the encrypted electronic data in a manner that the second computer does not use the specific apparatus number for the specific first computer in decrypting the encrypted electronic data.

30. The storage medium of claim 29, wherein the electronic information is software used for a computer.

31. The storage medium of claim 29, wherein the electronic information is electronically published information.

32. The storage medium of claim 29, wherein the storage medium is a read-only optical disk.

33. A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific first computer and which stores the encrypted decryption key onto the storage medium and which encrypts electronic data to be decrypted by a specific second computer based upon the decryption key and which stores the encrypted electronic data onto the storage medium, and accessible from a plurality of second computers which decrypt the encrypted decryption key stored on the storage medium based upon the medium personal number and independent from a specific apparatus number for the specific second computer and which decrypt encrypted electronic data stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific second computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing the encrypted electronic data and the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from the specific apparatus number for the specific second computer, and wherein the

encrypted decryption key and said medium personal number enables the second computer to decrypt the encrypted electronic data in a manner that the second computer does not use the specific apparatus number for the specific second computer in decrypting the encrypted electronic data.

34. A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific computer and which stores the encrypted decryption key onto the storage medium, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

a storage area for storing the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from the specific apparatus number for the specific computer; and

a storage area for storing encrypted electronic data to be decrypted by a user computer which is accessible after the decryption key has been decrypted, wherein said decryption key and said medium personal number enables the user computer to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted electronic data.

35. A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific

apparatus number for a specific computer and which stores the encrypted decryption key onto the storage medium and which encrypts electronic data to be decrypted by a user computer based upon the decryption key and which stores the encrypted electronic data onto the storage medium, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data and the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from the specific apparatus number for the specific computer, and wherein the encrypted decryption key and said medium personal number enables the user computer to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific first computer in decrypting the encrypted electronic data.

36. A storage medium accessible from a plurality of computers which decrypt an encrypted decryption key stored on the storage medium, the encrypted decryption key being based upon the medium personal number and independent from a specific apparatus number for a specific computer and which enables a user computer to decrypt encrypted electronic data stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific computer in a particular computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable from the computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

a storage area for storing the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from the specific apparatus number for the specific computer; and

a storage area for storing encrypted electronic data which is accessible after the decryption key has been decrypted, wherein said decryption key and said medium personal number enables the user computer to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific first computer in decrypting the encrypted electronic data.

37. A storage medium accessible from a vendor computer and a user computer at different times, the storage medium comprising:

a storage area for storing a medium personal number, which is un-rewritable from the computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

a storage area for storing an encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from a specific apparatus number for a specific computer; and

a storage area for storing encrypted electronic data to be decrypted by the user computer which is accessible after the decryption key has been decrypted, wherein said decryption key and said medium personal number enables the user computer to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific first computer in decrypting the encrypted electronic data.

38. A storage medium accessed by a vendor computer and a user computer, said storage medium, comprising:

a storage area for storing a medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

a storage area for storing an encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from a specific apparatus number for a specific computer; and

a storage area for storing encrypted electronic data to be decrypted by the user computer which is accessible after the decryption key has been decrypted, wherein said decryption key and said medium personal number enables the user computer to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific first computer in decrypting the encrypted electronic data.

39. A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific

apparatus number for a specific first computer and which stores the encrypted decryption key onto the storage medium, and accessible from a plurality of second computers which decrypt the encrypted decryption key stored on the storage medium based upon the medium personal number and independent from a specific apparatus number for a specific second computer and which decrypt encrypted electronic data stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific second computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data to be decrypted by the second computer, which includes data encrypted based upon the medium personal number and encrypted independent from the specific apparatus number for the specific first computer,

wherein the second computer decrypts encrypted electronic data in a manner that the second computer does not use the specific apparatus number for the specific first computer in decrypting the encrypted decryption key and the encrypted electronic data.

40. The storage medium of claim 39, wherein the electronic information is software used for a computer.

41. The storage medium of claim 39, wherein the electronic information is electronically published information.

42. The storage medium of claim 39, wherein the storage medium is a read-only optical disk.

43. A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific first computer and which stores the encrypted decryption key onto the storage medium and which encrypts electronic data based upon the decryption key and which stores the encrypted electronic data onto the storage medium, and accessible from a plurality of second computers which decrypt the encrypted decryption key stored on the storage medium based upon the medium personal number and independent from a specific apparatus number for a specific second computer and which decrypt encrypted electronic data stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific second computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data to be decrypted by the second computer, which includes information encrypted based upon the medium

personal number and encrypted independent from the specific apparatus number for the specific second computer,

wherein the second computer decrypts encrypted electronic data in a manner that the second computer does not use the specific apparatus number for the specific second computer in decrypting the encrypted electronic data.

44. A storage medium accessible from a vendor computer and a user computer, where the vendor computer encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific computer and which stores the encrypted decryption key onto the storage medium, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data to be decrypted by the user computer wherein the encrypted electronic data includes information encrypted based upon the medium personal number and encrypted independent from the specific apparatus number for the specific computer,

wherein said user computer decrypts the encrypted electronic data in a manner that the second computer does not use the specific apparatus number for the specific second computer in decrypting the encrypted electronic data.

45. A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific computer and which stores the encrypted decryption

key onto the storage medium and which encrypts electronic data to be decrypted by a user computer based upon the decryption key and which stores the encrypted electronic data onto the storage medium, the storage medium comprising:

a storage area for storing a medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data wherein the encrypted electronic data includes information encrypted based upon the medium personal number and encrypted independent from the specific apparatus number for the specific computer,

wherein the user computer decrypts the encrypted electronic data in a manner that the second computer does not use the specific apparatus number for the specific second computer in decrypting the encrypted electronic data.

46. A storage medium accessible from a plurality of computers which decrypt an encrypted decryption key stored on the storage medium, the encrypted decryption key being based upon the medium personal number and independent from a specific apparatus number for a specific computer and which decrypt encrypted electronic data stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific computer in a particular computer, comprising:

a storage area for storing the medium personal number, which is un-rewritable from the computers, wherein the medium personal number is particularly personal for

each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data to be decrypted by a user computer wherein the encrypted electronic data includes information encrypted based upon the medium personal number and encrypted independent from the specific apparatus number for the specific computer,

wherein the user computer decrypts encrypted electronic data in a manner that the second computer does not use the specific apparatus number for the specific second computer in decrypting the encrypted electronic data.

47. A storage medium accessible from different computers at different times, the storage medium comprising:

a storage area for storing a medium personal number, which is un-rewritable from the computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

a storage area for storing encrypted electronic data to be decrypted by a user computer, which includes information encrypted based upon the medium personal number and encrypted independent from a specific apparatus number for a specific computer; and

a storage area for storing electronic data which is accessible after the encrypted electronic data has been decrypted,

wherein the medium personal number enables a user computer to decrypt the encrypted electronic data in a manner that the user computer does not use the specific

apparatus number for the specific computer in decrypting the encrypted decryption key encrypted electronic data.

48. A storage medium accessed by a vendor computer and a user computer, said storage medium comprising:

a storage area for storing a medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

a storage area for storing encrypted electronic data to be decrypted by the user computer which includes information encrypted based upon the medium personal number and encrypted independent from a specific apparatus number for a specific computer; and

a storage area for storing electronic data which is accessible after the encrypted electronic data has been decrypted,

wherein the medium personal number enables the user computer to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted decryption key encrypted electronic data.

49. A storage medium accessed by a vendor computer and a user computer in a manner such that a decryption key is encrypted based upon a medium personal number and independent from a specific apparatus number for a specific computer and the encrypted decryption key is stored onto the storage medium, and accessed in a manner such that the encrypted decryption key stored on the storage medium is decrypted based upon the medium personal number and independent from the specific apparatus

number for the specific computer and that encrypted electronic data stored on the storage medium is decrypted based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data to be decrypted by the user computer, wherein the encrypted electronic data includes information encrypted based upon the medium personal number and encrypted independent from the specific apparatus number for the specific computer,

wherein the decryption key and said medium personal number enables the user computer to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted decryption key encrypted electronic data.

50. The storage medium of claim 49, wherein the electronic information is software used for a computer.

51. The storage medium of claim 49, wherein the electronic information is electronically published information.

52. The storage medium of claim 49, wherein the storage medium is a read-only optical disk.

53. A storage medium accessed by a vendor computer and a user computer in a manner such that a decryption key is decrypted based upon a medium personal number

and independent from a specific apparatus number for a specific computer and the encrypted decryption key is stored onto the storage medium and that electronic data is encrypted based upon the decryption key and the encrypted electronic data is stored onto the storage medium, and accessed in a manner such that the encrypted decryption key stored on the storage medium is decrypted based upon the medium personal number and independent from the specific apparatus number for the specific computer and that the encrypted electronic information stored on the storage medium is decrypted based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific computer in a particular second computer in different time, the storage medium comprising:

a storage area for storing a medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data to be decrypted by the user computer, wherein the encrypted electronic data includes information encrypted based upon the medium personal number and encrypted independent from the specific apparatus number for the specific computer,

wherein the decryption key and said medium personal number enables the user computer to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted decryption key encrypted electronic data.

54. A storage medium accessed by a vendor computer and a user computer in a manner such that a decryption key is encrypted based upon a medium personal number

and independent from a specific apparatus number for a specific computer and that the encrypted decryption key is stored onto the storage medium, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data to be decrypted by the user computer, wherein the encrypted electronic data includes information encrypted based upon the medium personal number and encrypted independent from the specific apparatus number for the specific computer,

wherein the decryption key and said medium personal number enables the user computer to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted decryption key encrypted electronic data.

55. A storage medium accessed by a vendor computer and a user computer in a manner such that a decryption key is encrypted based upon a medium personal number and independent from a specific apparatus number for a specific computer and the encrypted decryption key is stored onto the storage medium and that electronic data is encrypted based upon the decryption key and the encrypted electronic data is stored onto the storage medium, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data to be decrypted by the user computer, wherein the encrypted electronic data includes information encrypted based upon the medium personal number and encrypted independent from the specific apparatus number for the specific computer,

wherein the decryption key and said medium personal number enables the user computer to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted decryption key encrypted electronic data.

56. A storage medium accessed by a vendor computer and a user computer in a manner such that an encrypted decryption key stored on the storage medium is decrypted based upon a medium personal number and independent from a specific apparatus number for a specific computer and encrypted electronic data stored on the storage medium is decrypted based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data to be decrypted by the user computer, wherein the encrypted electronic data includes information encrypted based upon the medium personal number and encrypted independent from the specific apparatus number for the specific computer,

wherein the decryption key and said medium personal number enables the user computer to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted decryption key encrypted electronic data.

111. A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

an area storing encrypted electronic data to be decrypted by the user computer;

an area storing a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which the user computer cannot change; and

an area storing permission information which includes a decryption key encrypted in a manner that is independent from a specific apparatus number for a specific computer and based upon said medium personal number, wherein said permission information and said medium personal number enabling the user computer to decrypt the encrypted decryption key and to decrypt the encrypted electronic data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted decryption key and the encrypted electronic data.

112. A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

an area storing encrypted electronic data to be decrypted by the user computer;

an area storing a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which the user computer cannot rewrite; and

wherein the user computer decrypts the encrypted electronic data using permission information which is encrypted in a manner that is independent from a specific apparatus number for a specific computer and based upon said medium personal number.

113. A storage medium accessed by a vendor computer and a user computer said storage medium for storing information readable by said user computer, said storage medium comprising:

an area storing encrypted electronic data to be decrypted by the user computer;

an area storing a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

wherein the user computer decrypts the encrypted electronic data using permission information that is encrypted independent from a specific apparatus number for a specific computer;

wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which a user computer cannot rewrite.

114. A storage medium readable by a device, the storage medium comprising:

encrypted data; and

first data that is based on a medium personal number and not based on a specific device identifier for a specific device, wherein the medium personal number is un-rewritable and unique to the storage medium, and wherein the first data is used by the device to decrypt the encrypted data.

115. A storage medium according to claim 114, wherein the first data includes a key encrypted based on the medium personal number.

116. A storage medium according to claim 114, wherein the encrypted data is encrypted based on the key.

117. A storage medium according to claim 114, wherein the first data comprises the medium personal number.

118. A storage medium readable by different devices at different times, the storage medium comprising:

encrypted data; and

first data that is based on a medium personal number and not based on a specific device identifier for a specific device, wherein the medium personal number is un-rewritable and unique to the storage medium, and wherein the first data is used by

the device to decrypt the encrypted data.

119. A storage medium readable by a vendor computer and a user computer, said storage medium comprising:

data representing a medium personal number;

encrypted electronic data to be decrypted by the user computer; and

first data that is based on the medium personal number and encrypted independent from a specific apparatus number for a specific computer, wherein the medium personal number is un-rewritable and particularly personal for each storage medium and is different from a medium personal number of another storage medium, and wherein the user computer decrypts the encrypted electronic data using the first data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted electronic data.

120. A storage medium according to claim 119, wherein the first data includes a key encrypted based on the medium personal number.

121. A storage medium according to claim 119, wherein the encrypted data is encrypted based on the key.

122. A storage medium according to claim 119, wherein the first data comprises the medium personal number.

123. A storage medium readable by a vendor computer and a user computer at different times, the storage medium comprising:

data representing a medium personal number;

encrypted electronic data to be decrypted by the user computer; and

first data that is based on the medium personal number and encrypted independent from a specific apparatus number for a specific computer, wherein the medium personal number is un-rewritable and particularly personal for each storage medium and is different from a medium personal number of another storage medium, and wherein the user computer decrypts the encrypted electronic data using the first data in a manner that the user computer does not use the specific apparatus number for the specific computer in decrypting the encrypted electronic data.

124. A storage medium for storing data for access and processing by a vendor computer and a user computer, said storage medium comprising:

a medium personal number storage area including a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein the medium personal number is written onto the storage medium in an un-rewritable form which a user storage reading apparatus cannot rewrite;

an electronic information storage area including encrypted electronic data to be decrypted by the user computer; and

the user computer decrypts the encrypted electronic data based upon an encrypted decryption key which has been encrypted based on said medium personal number and encrypted independent from a specific apparatus number for a specific computer.

125. A storage medium for storing data for access and processing by a vendor computer and a user computer, said storage medium comprising:

an encrypted electronic data storage area including encrypted electronic data to be decrypted by the user computer;

a medium personal number storage area including a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which the user storage reading apparatus cannot rewrite, and said medium personal number enables decrypting of said encrypted electronic data from the user computer; and

wherein the user computer decrypts the encrypted electronic data based upon information which is encrypted based on said medium personal number and encrypted independent from a specific apparatus number for a specific computer.

APPENDIX 2

DRAWINGS OF APPLICATION SERIAL NO. 09/476,319

Fig. 1

PRIOR ART

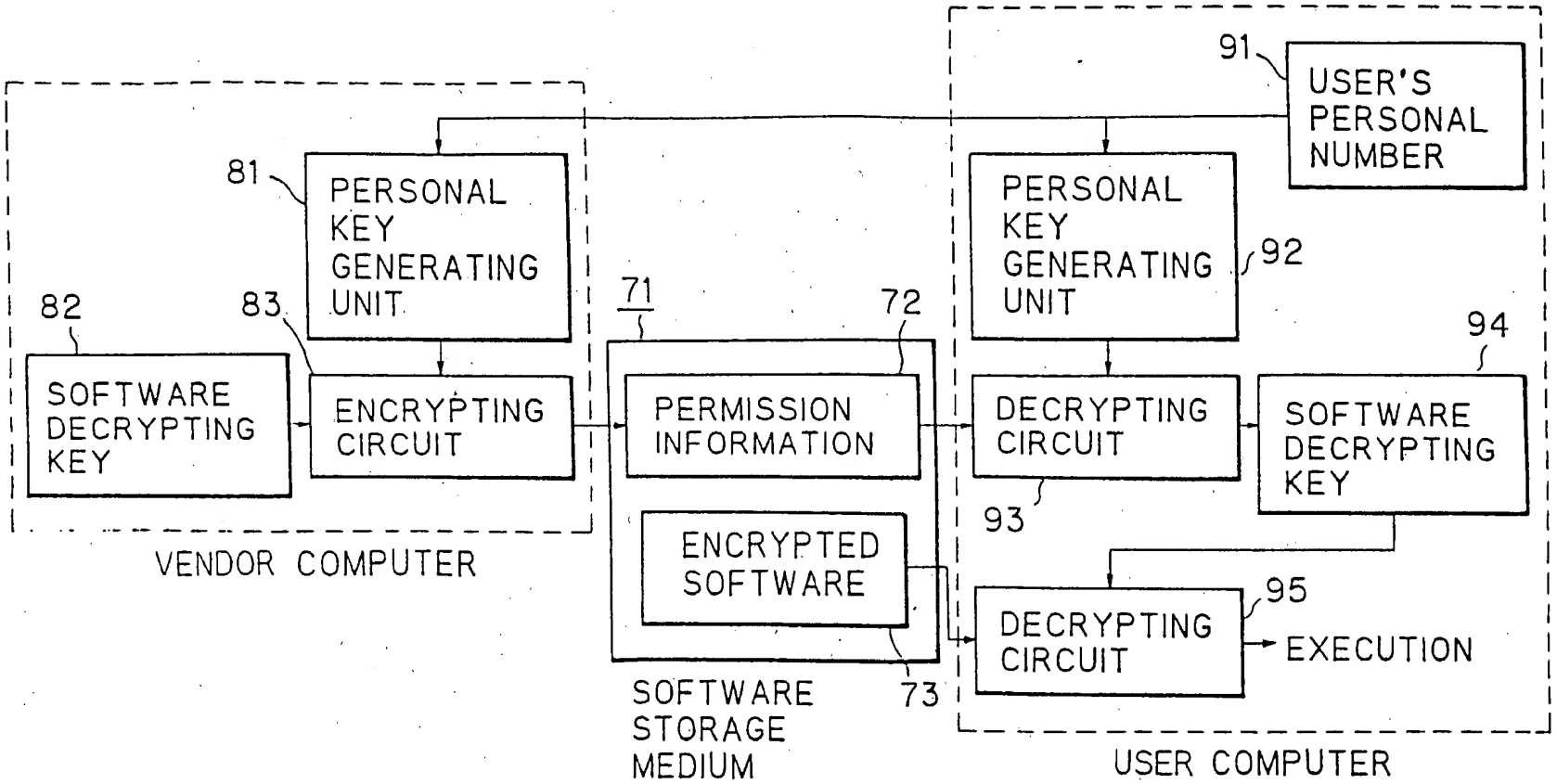


Fig. 2

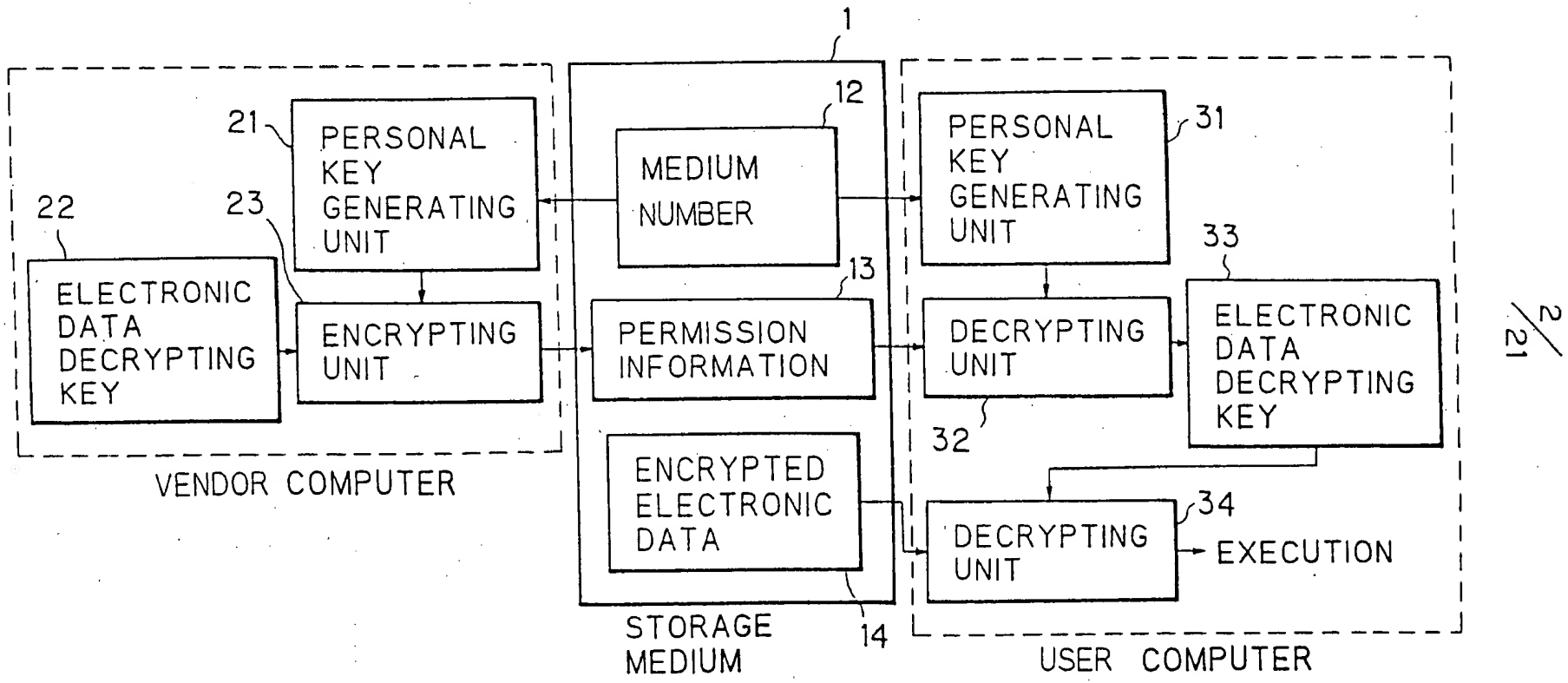

1
12
21
PERSONAL KEY GENERATING UNIT
MEDIUM NUMBER
PERSONAL KEY GENERATING UNIT
31
22
23
ELECTRONIC DATA DECRYPTING KEY
ENCRYPTING UNIT
13
PERMISSION INFORMATION
DECRYPTING UNIT
33
ELECTRONIC DATA DECRYPTING KEY
32
VENDOR COMPUTER
ENCRYPTED ELECTRONIC DATA
34
DECRYPTING UNIT
EXECUTION
STORAGE MEDIUM
14
USER COMPUTER

Fig. 3

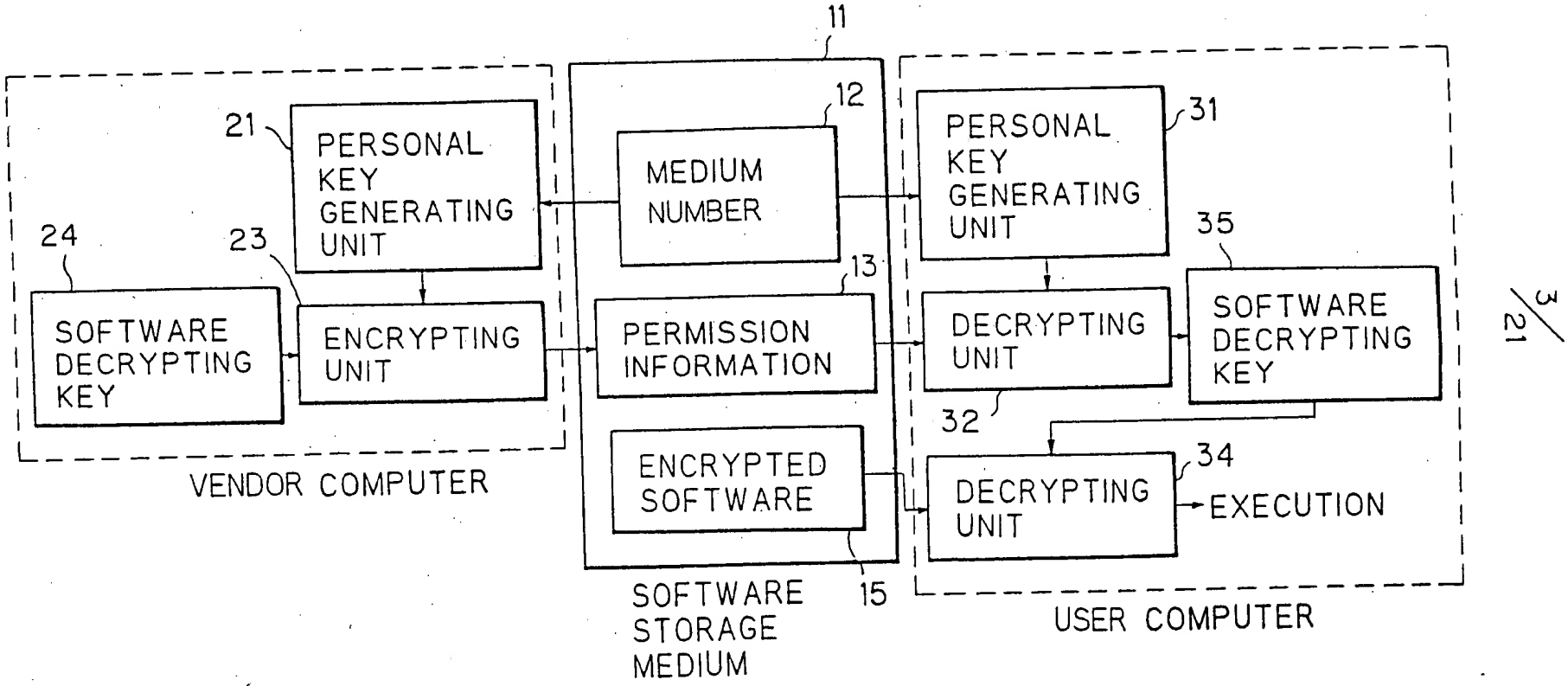

11
12
21
PERSONAL KEY GENERATING UNIT
MEDIUM NUMBER
31
PERSONAL KEY GENERATING UNIT
24
23
35
SOFTWARE DECRYPTING KEY
ENCRYPTING UNIT
13
PERMISSION INFORMATION
DECRYPTING UNIT
SOFTWARE DECRYPTING KEY
32
34
ENCRYPTED SOFTWARE
DECRYPTING UNIT
EXECUTION
VENDOR COMPUTER
SOFTWARE STORAGE MEDIUM
15
USER COMPUTER

Fig. 4

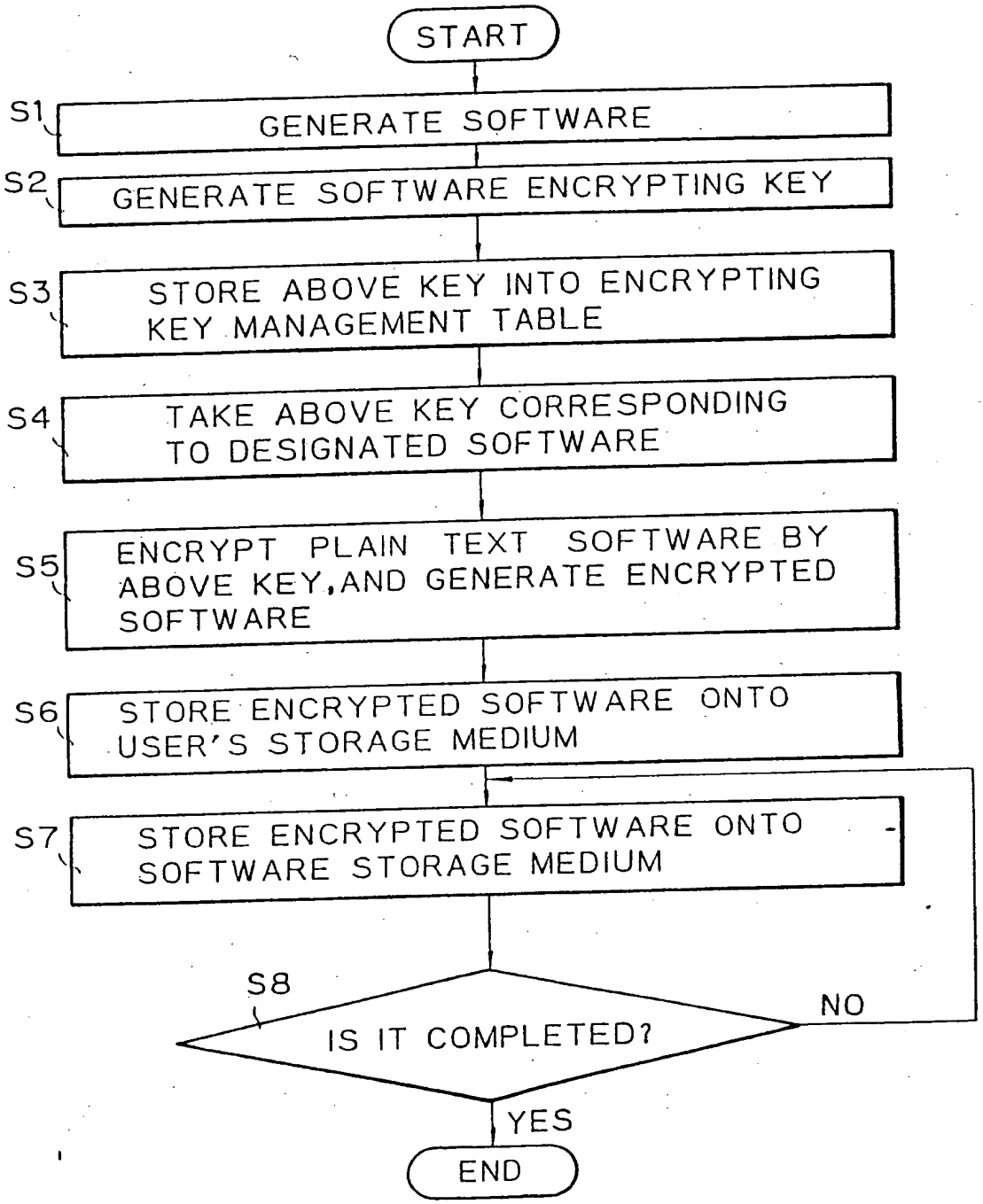

START
S1
GENERATE SOFTWARE
S2
GENERATE SOFTWARE ENCRYPTING KEY
S3
STORE ABOVE KEY INTO ENCRYPTING KEY MANAGEMENT TABLE
S4
TAKE ABOVE KEY CORRESPONDING TO DESIGNATED SOFTWARE
S5
ENCRYPT PLAIN TEXT SOFTWARE BY ABOVE KEY, AND GENERATE ENCRYPTED SOFTWARE
S6
STORE ENCRYPTED SOFTWARE ONTO USER'S STORAGE MEDIUM
S7
STORE ENCRYPTED SOFTWARE ONTO SOFTWARE STORAGE MEDIUM
S8
IS IT COMPLETED?
NO
YES
END

Fig. 5A

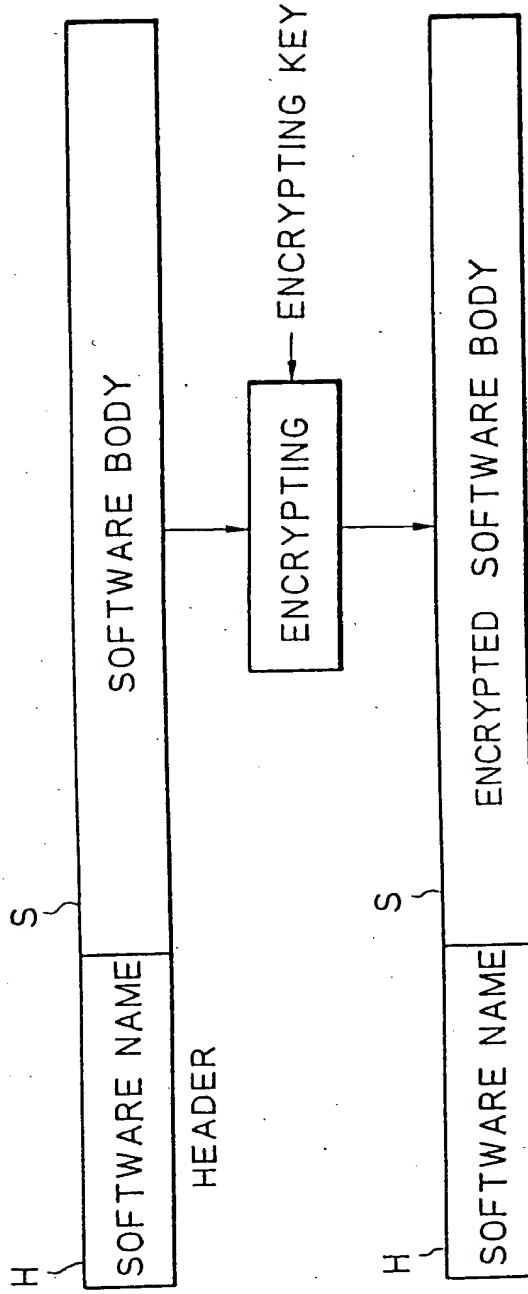

SOFTWARE BODY
SOFTWARE NAME
HEADER
S
H
ENCRYPTING KEY
ENCRYPTING
ENCRYPTED SOFTWARE BODY
SOFTWARE NAME
HEADER
S
H

Fig. 5B

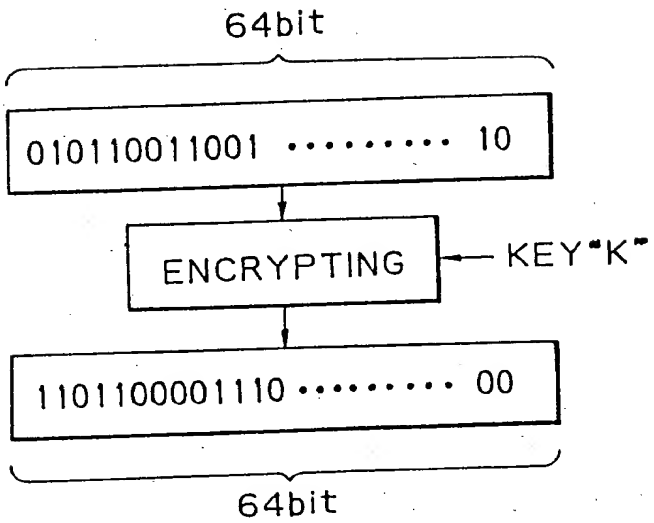

64bit
010110011001 ····· 10
ENCRYPTING
KEY"K"
1101100001110 ····· 00
64bit

Fig. 6

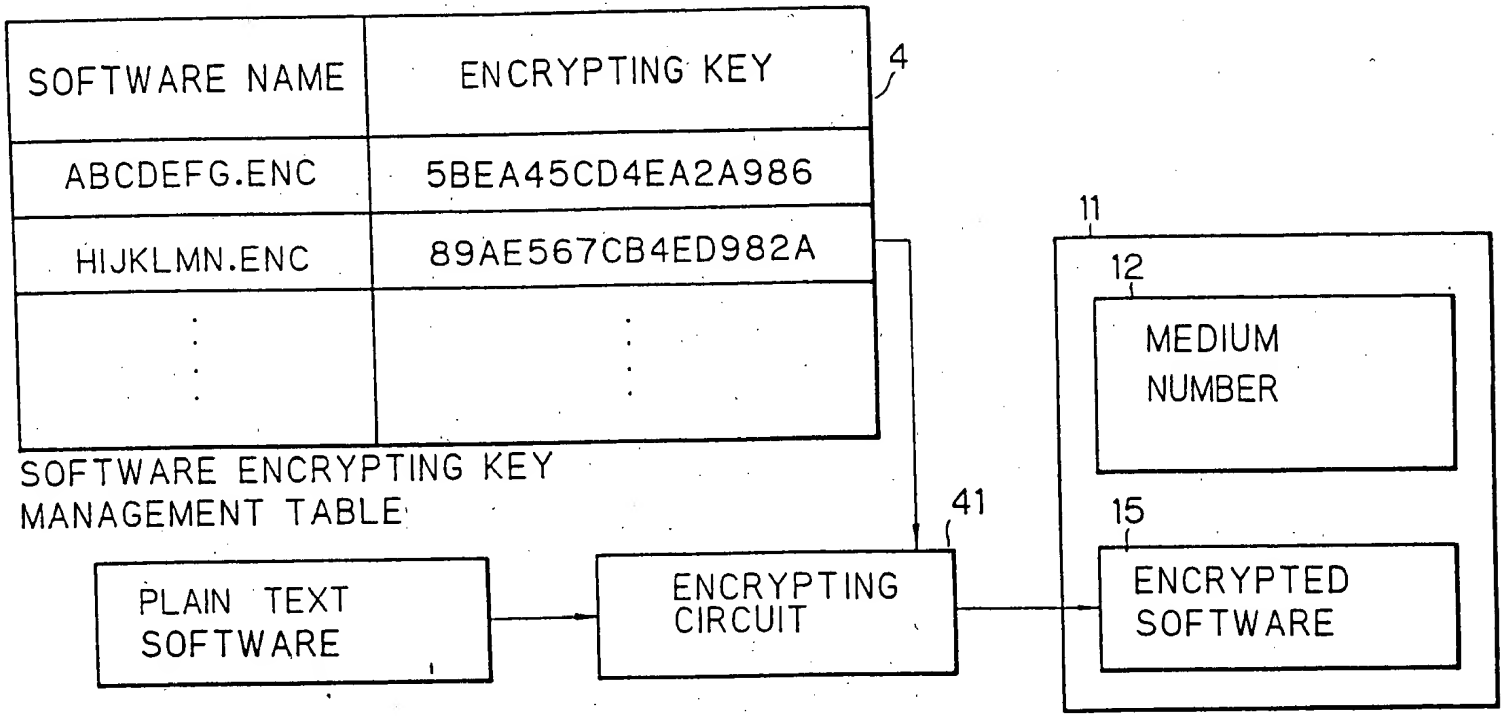

SOFTWARE NAME
ENCRYPTING KEY
4
ABCDEFG.ENC
5BEA45CD4EA2A986
HIJKLMN.ENC
89AE567CB4ED982A
SOFTWARE ENCRYPTING KEY MANAGEMENT TABLE
11
12
MEDIUM NUMBER
41
15
PLAIN TEXT SOFTWARE
ENCRYPTING CIRCUIT
ENCRYPTED SOFTWARE

Fig. 7A

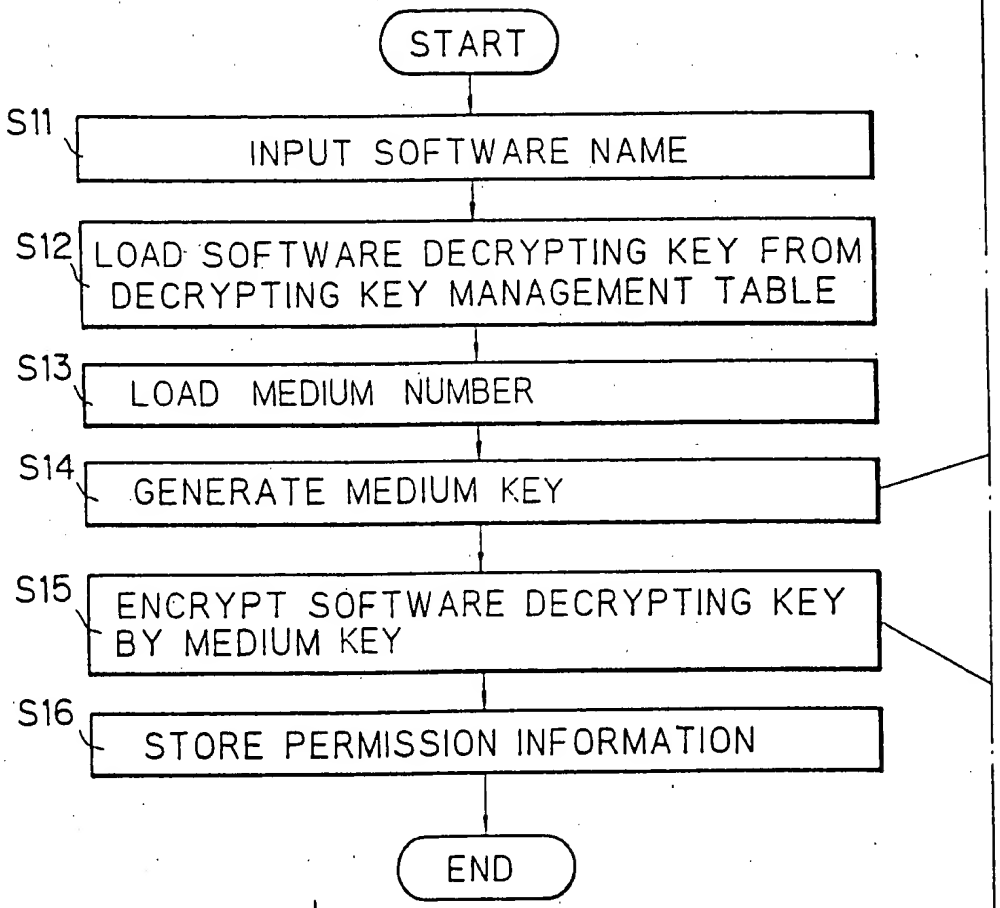


Fig.7

Fig.7A	Fig.7B

Fig. 7B

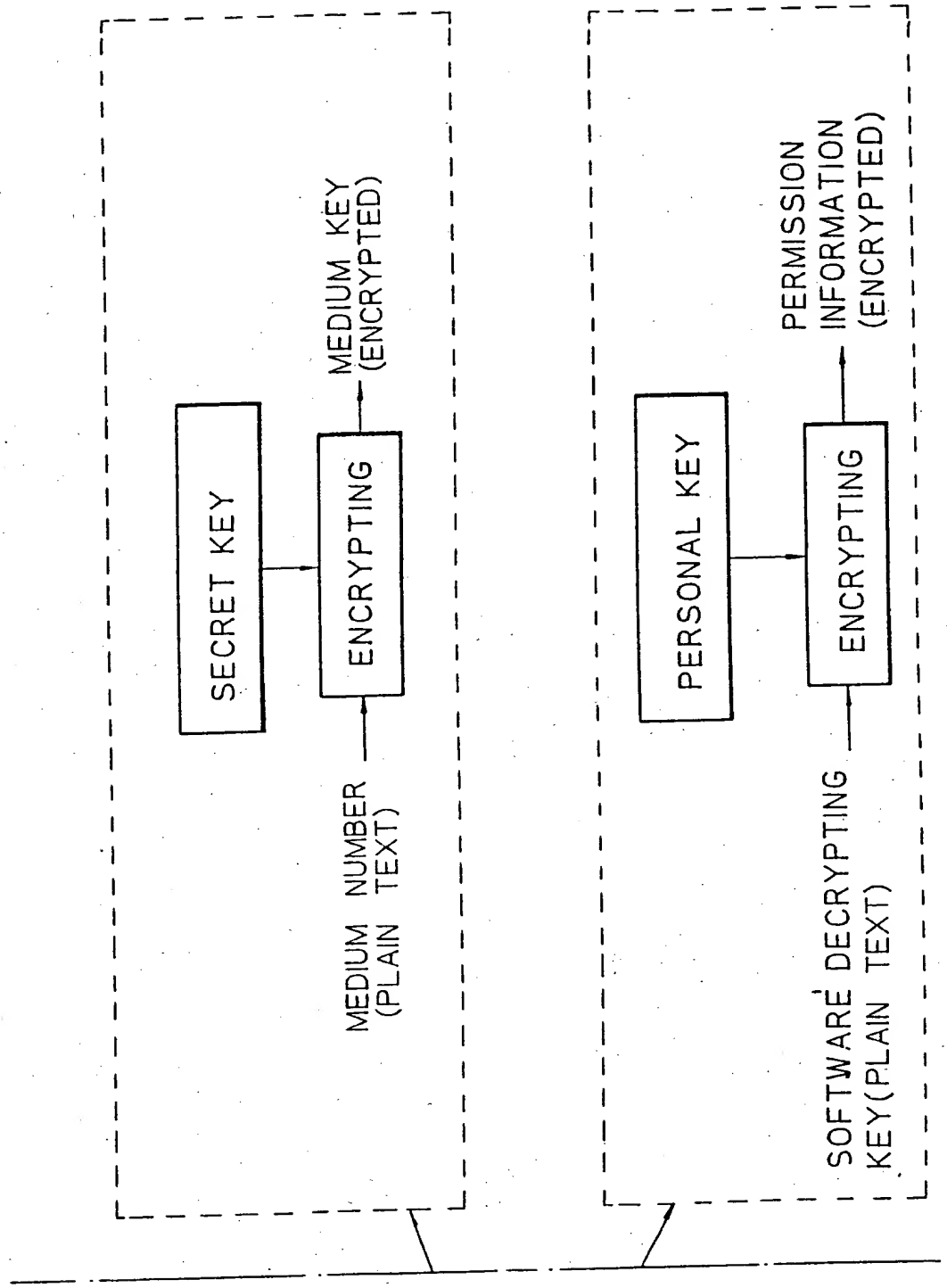

SECRET KEY
ENCRYPTING
MEDIUM KEY (ENCRYPTED)
MEDIUM NUMBER (PLAIN TEXT)
PERSONAL KEY
ENCRYPTING
PERMISSION INFORMATION (ENCRYPTED)
SOFTWARE DECRYPTING KEY(PLAIN TEXT)

Fig. 8

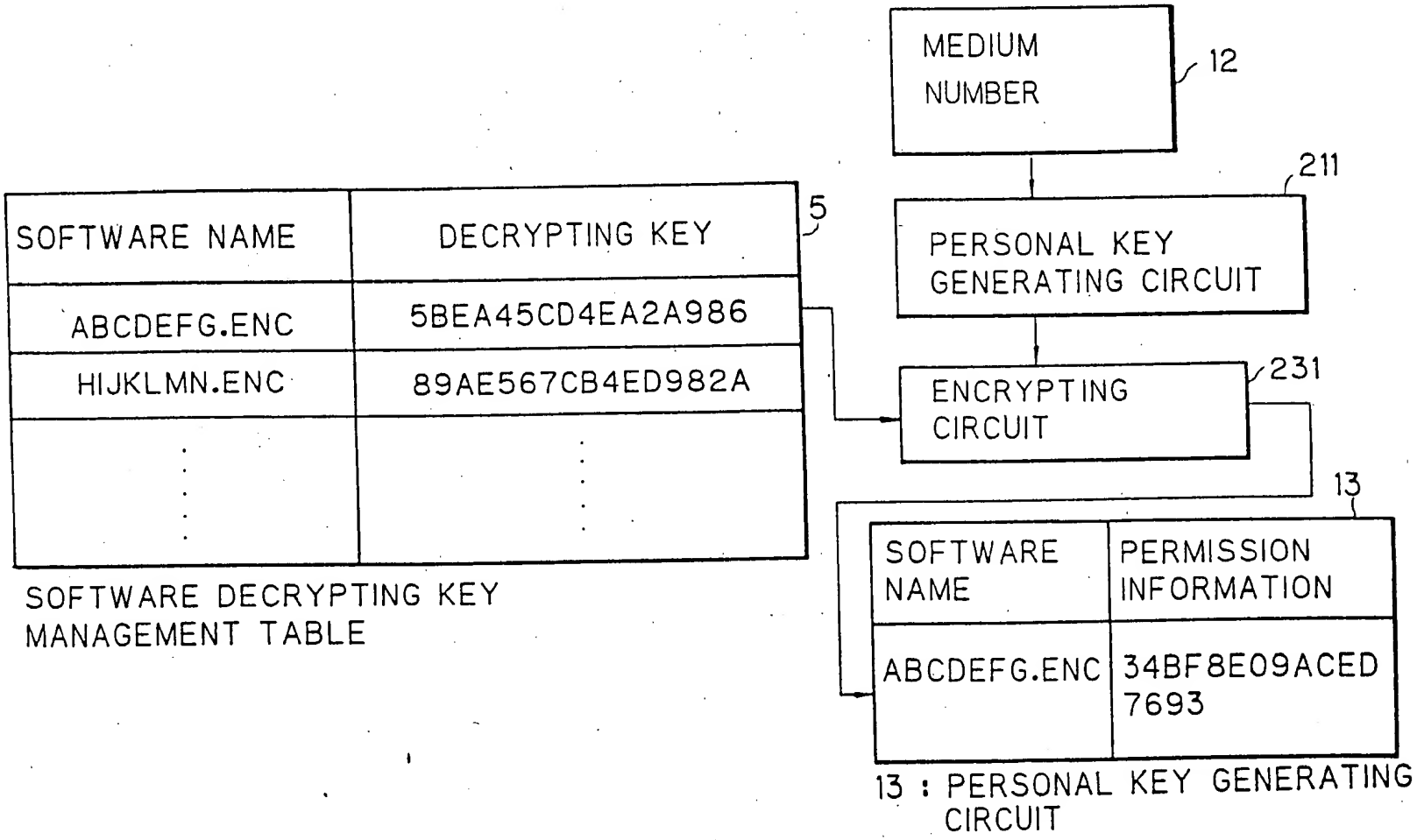

MEDIUM NUMBER
12
211
PERSONAL KEY GENERATING CIRCUIT
ENCRYPTING CIRCUIT
231
13
SOFTWARE NAME
DECRYPTING KEY
5
ABCDEFG.ENC
5BEA45CD4EA2A986
HIJKLMN.ENC
89AE567CB4ED982A
SOFTWARE DECRYPTING KEY MANAGEMENT TABLE
SOFTWARE NAME
PERMISSION INFORMATION
ABCDEFG.ENC
34BF8E09ACED7693
13 : PERSONAL KEY GENERATING CIRCUIT

Fig. 9A

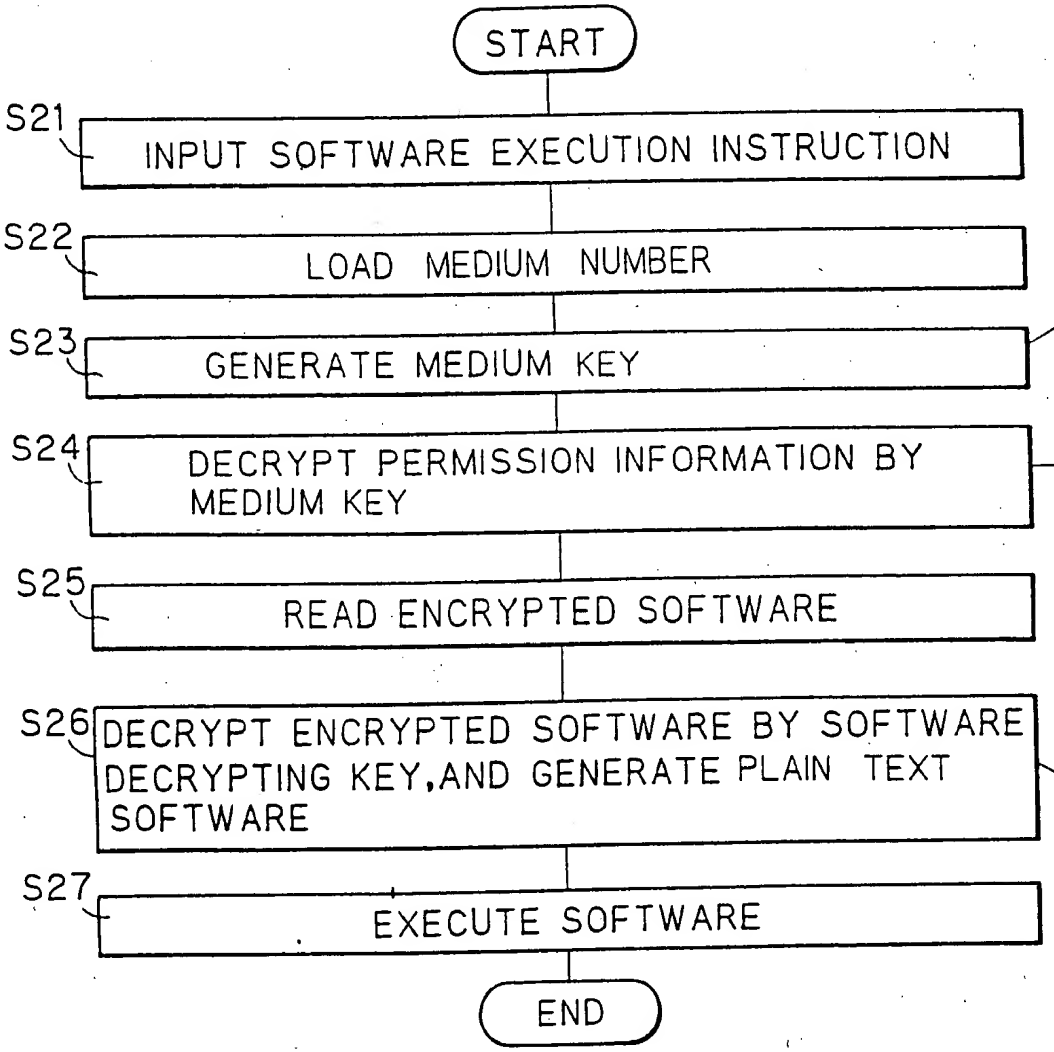


Fig.9

Fig.9A	Fig.9B

Fig. 9B

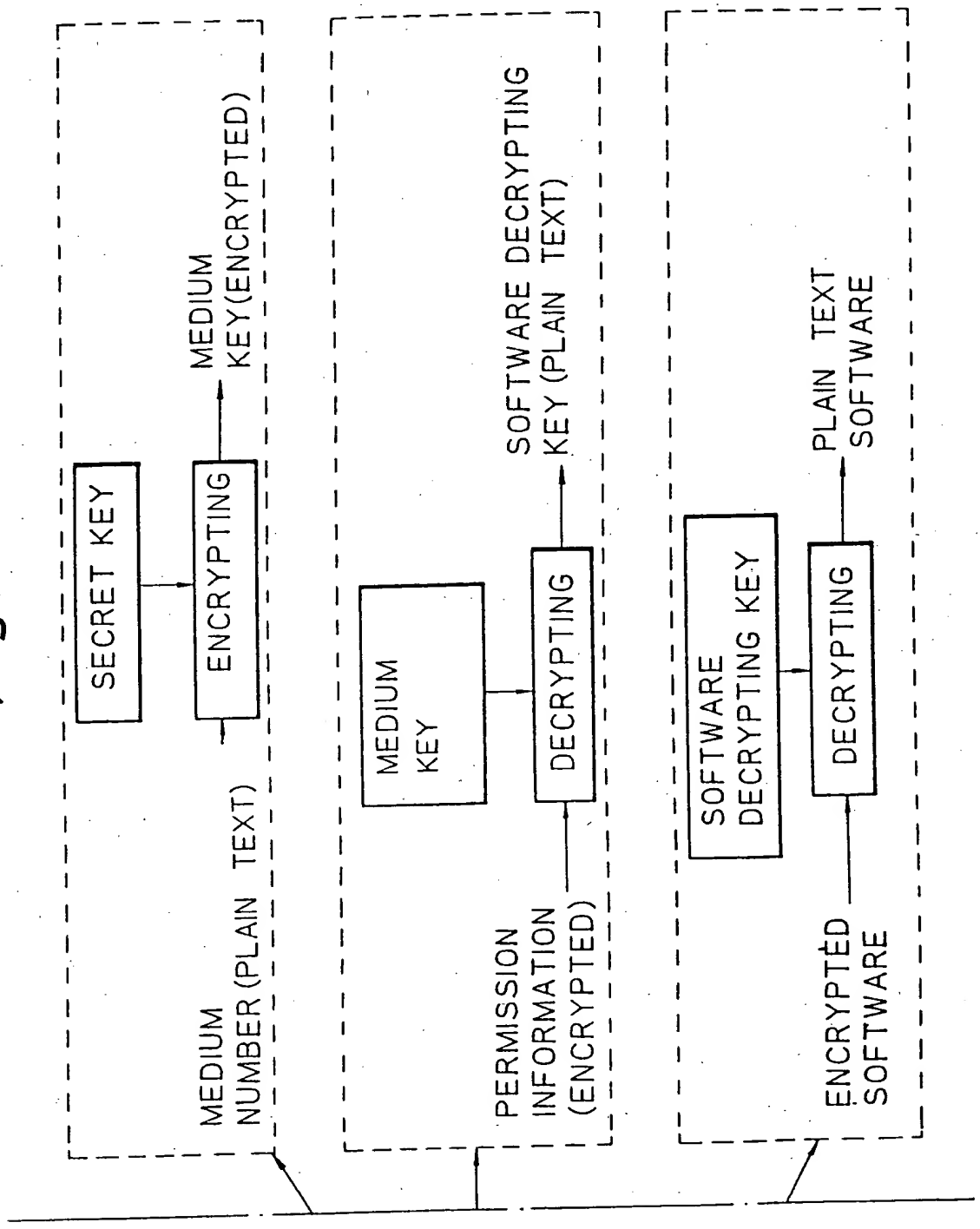

SECRET KEY
ENCRYPTING
MEDIUM KEY(ENCRYPTED)
MEDIUM NUMBER (PLAIN TEXT)
MEDIUM KEY
DECRYPTING
SOFTWARE DECRYPTING KEY (PLAIN TEXT)
PERMISSION INFORMATION (ENCRYPTED)
SOFTWARE DECRYPTING KEY
DECRYPTING
PLAIN TEXT SOFTWARE
ENCRYPTED SOFTWARE

Fig. 10A

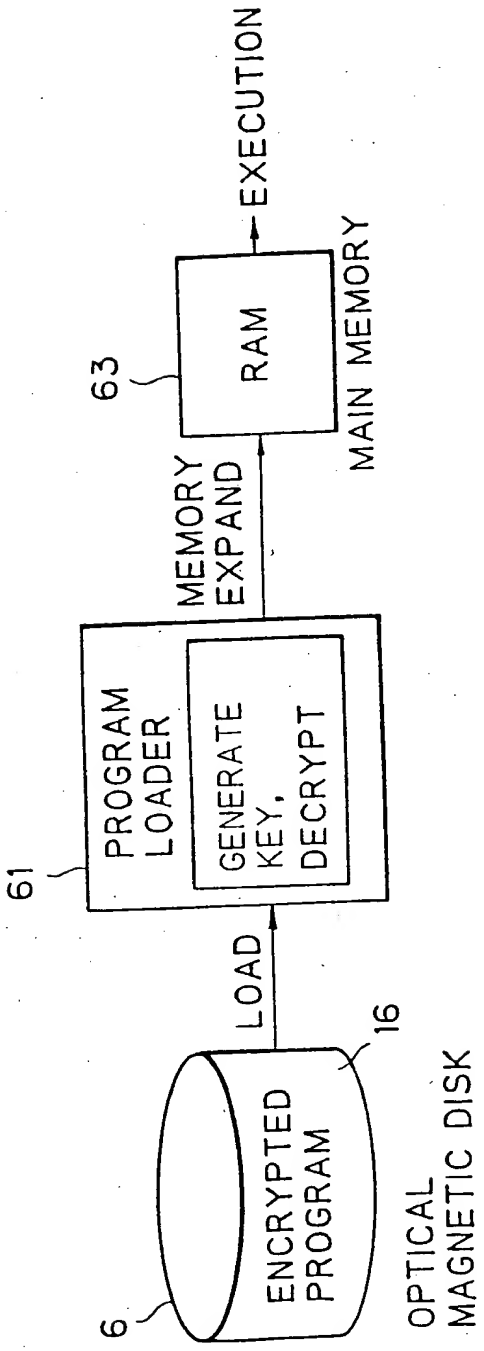

EXECUTION
MAIN MEMORY
63
RAM
MEMORY EXPAND
61
PROGRAM LOADER
GENERATE KEY, DECRYPT
LOAD
16
ENCRYPTED PROGRAM
6
OPTICAL MAGNETIC DISK

Fig. 10B

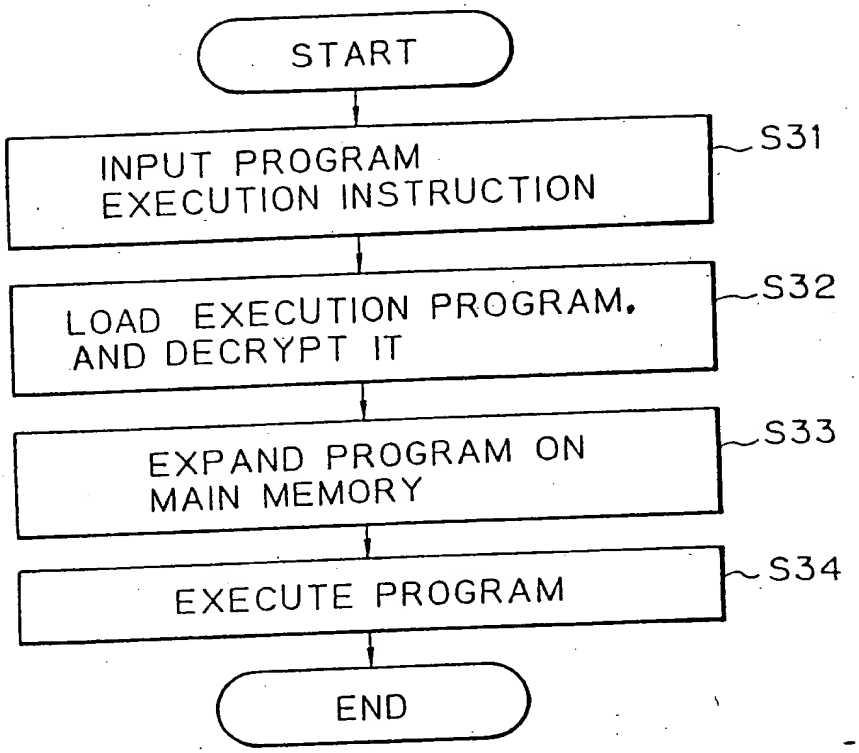

START
INPUT PROGRAM EXECUTION INSTRUCTION
S31
LOAD EXECUTION PROGRAM, AND DECRYPT IT
S32
EXPAND PROGRAM ON MAIN MEMORY
S33
EXECUTE PROGRAM
S34
END

Fig. 10C

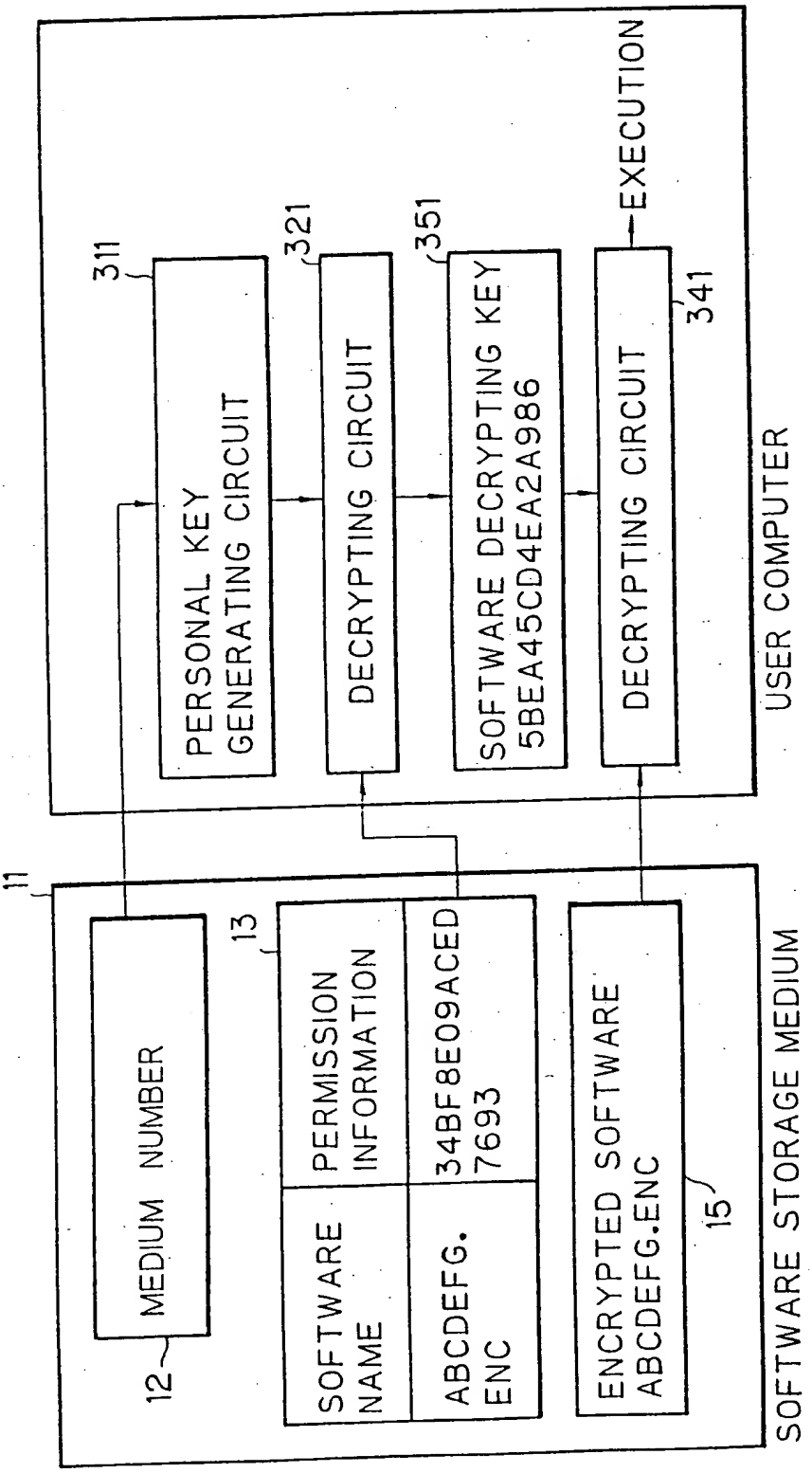

USER COMPUTER
311
PERSONAL KEY GENERATING CIRCUIT
321
DECRYPTING CIRCUIT
351
SOFTWARE DECRYPTING KEY 5BEA45CD4EA2A986
EXECUTION
341
DECRYPTING CIRCUIT
11
SOFTWARE STORAGE MEDIUM
12
MEDIUM NUMBER
13
PERMISSION INFORMATION
34BF8E09ACED 7693
SOFTWARE NAME
ABCDEFG. ENC
15
ENCRYPTED SOFTWARE ABCDEFG.ENC

Fig. 11A

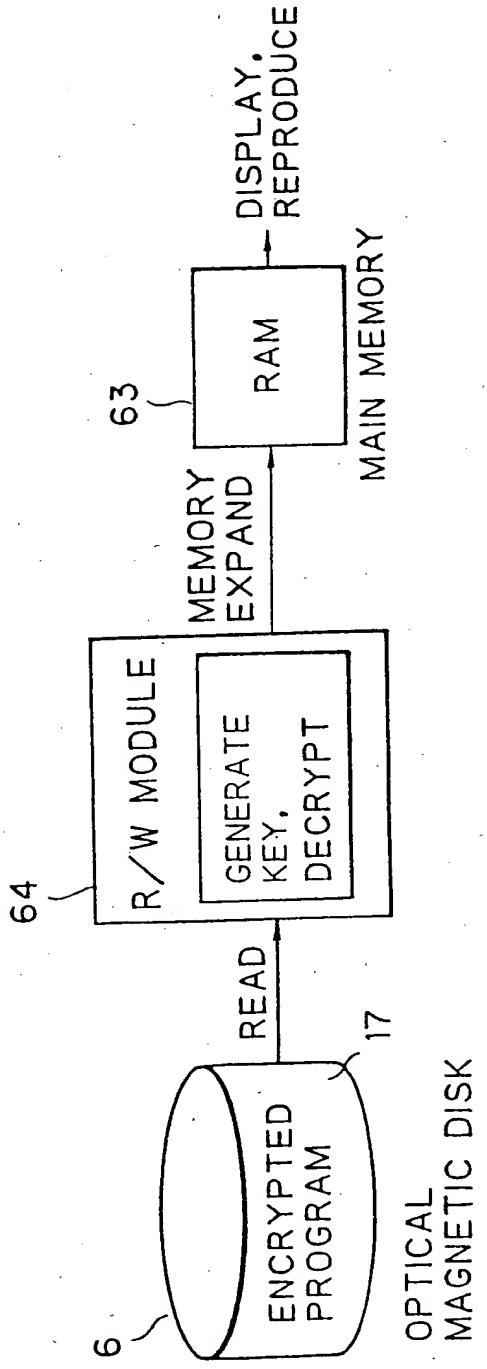

6
ENCRYPTED PROGRAM
17
OPTICAL MAGNETIC DISK
READ
64
R/W MODULE
GENERATE KEY, DECRYPT
MEMORY EXPAND
63
RAM
MAIN MEMORY
DISPLAY, REPRODUCE

Fig. 11B

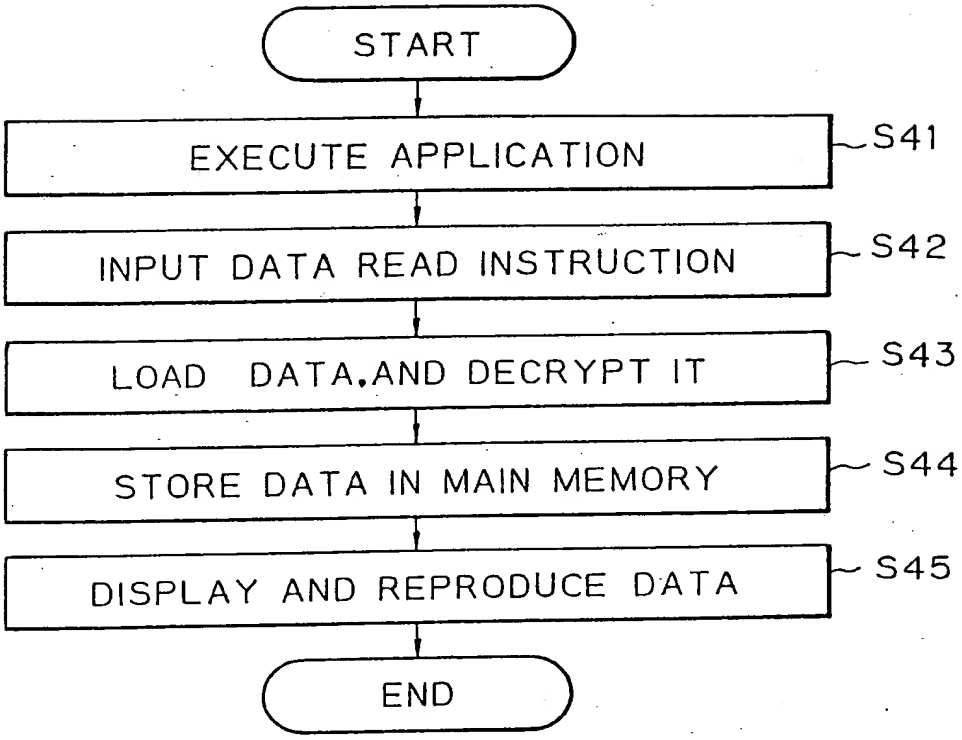

START
EXECUTE APPLICATION
S41
INPUT DATA READ INSTRUCTION
S42
LOAD DATA, AND DECRYPT IT
S43
STORE DATA IN MAIN MEMORY
S44
DISPLAY AND REPRODUCE DATA
S45
END

Fig. 11C

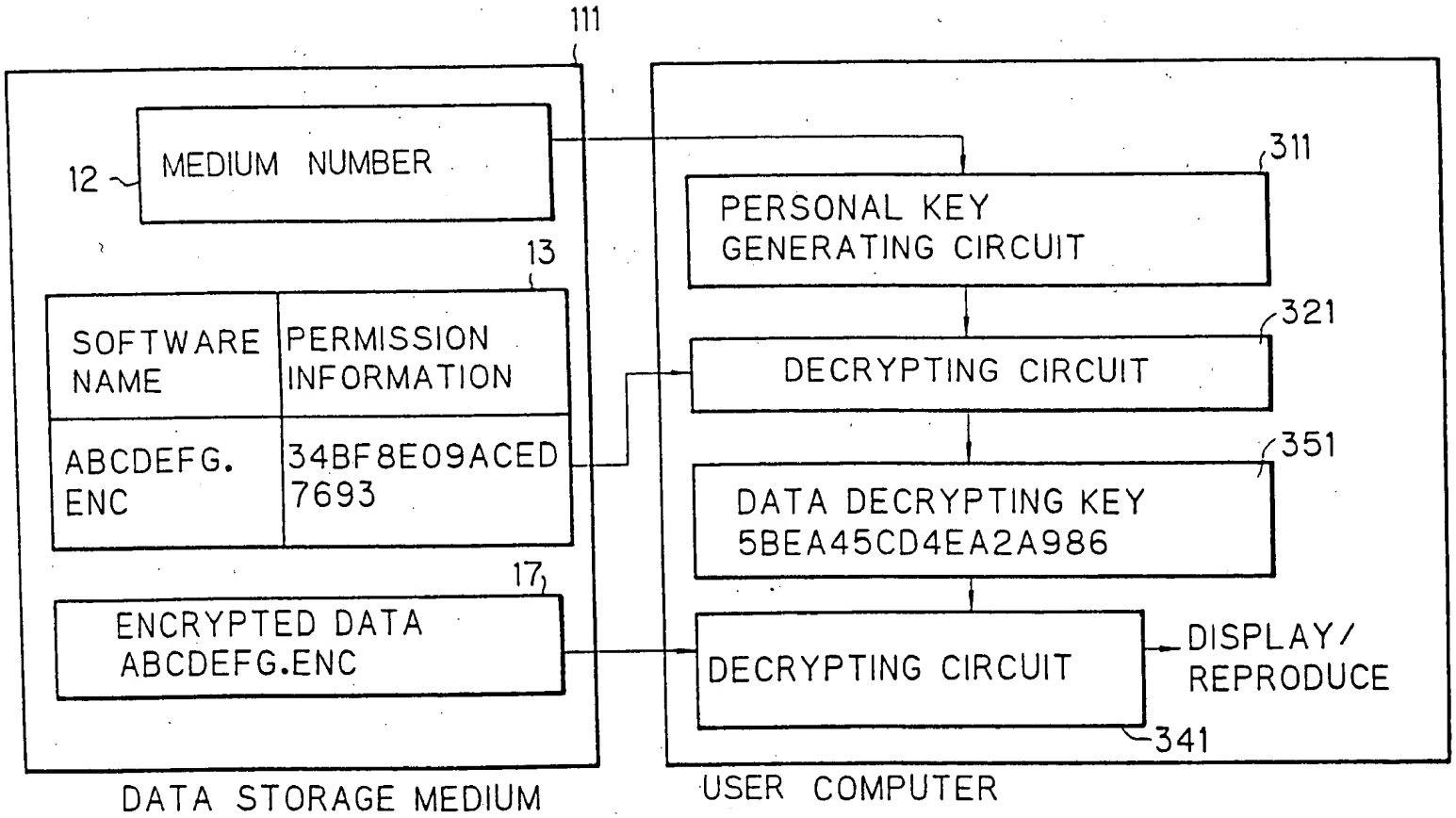

111
12
MEDIUM NUMBER
13
SOFTWARE NAME
PERMISSION INFORMATION
ABCDEFG. ENC
34BF8E09ACED 7693
17
ENCRYPTED DATA ABCDEFG.ENC
DATA STORAGE MEDIUM
311
PERSONAL KEY GENERATING CIRCUIT
321
DECRYPTING CIRCUIT
351
DATA DECRYPTING KEY 5BEA45CD4EA2A986
DECRYPTING CIRCUIT
341
DISPLAY/ REPRODUCE
USER COMPUTER

Fig. 12

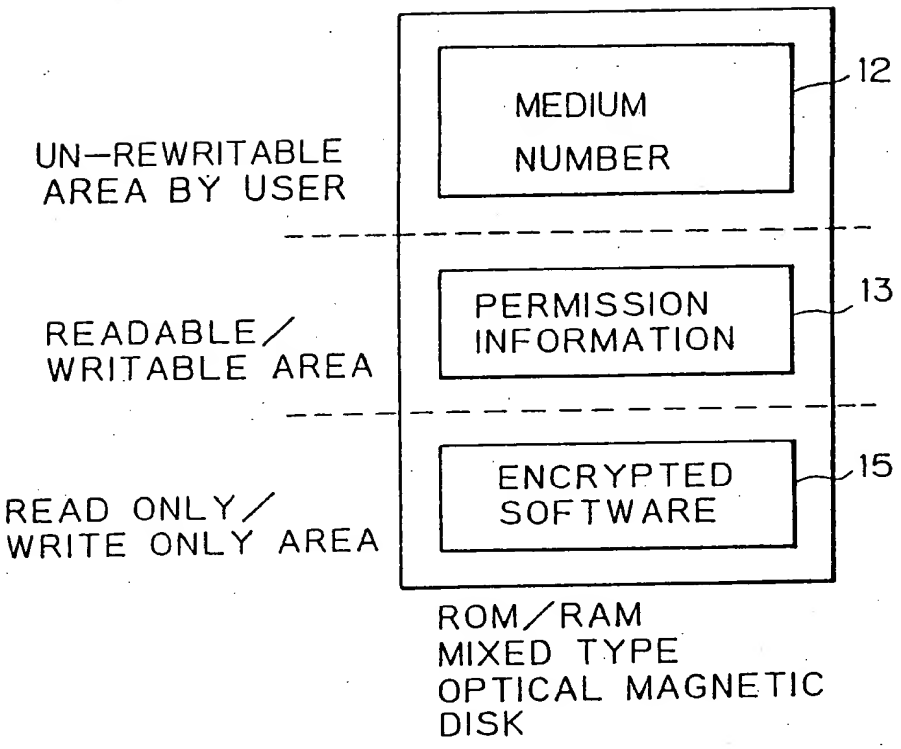

MEDIUM NUMBER
12
UN-REWRITABLE AREA BY USER
PERMISSION INFORMATION
13
READABLE/ WRITABLE AREA
ENCRYPTED SOFTWARE
15
READ ONLY/ WRITE ONLY AREA
ROM/RAM MIXED TYPE OPTICAL MAGNETIC DISK

Fig. 13

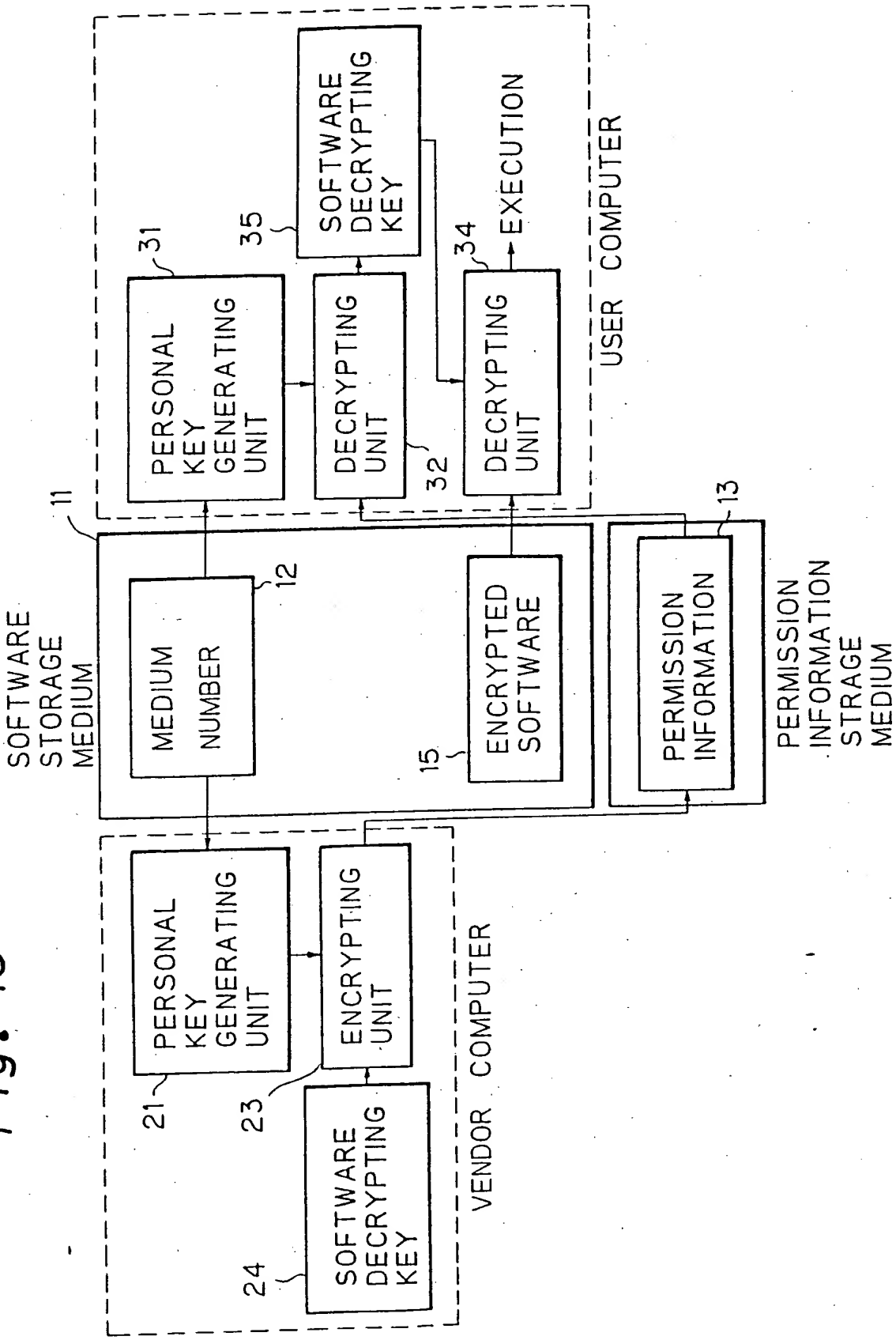
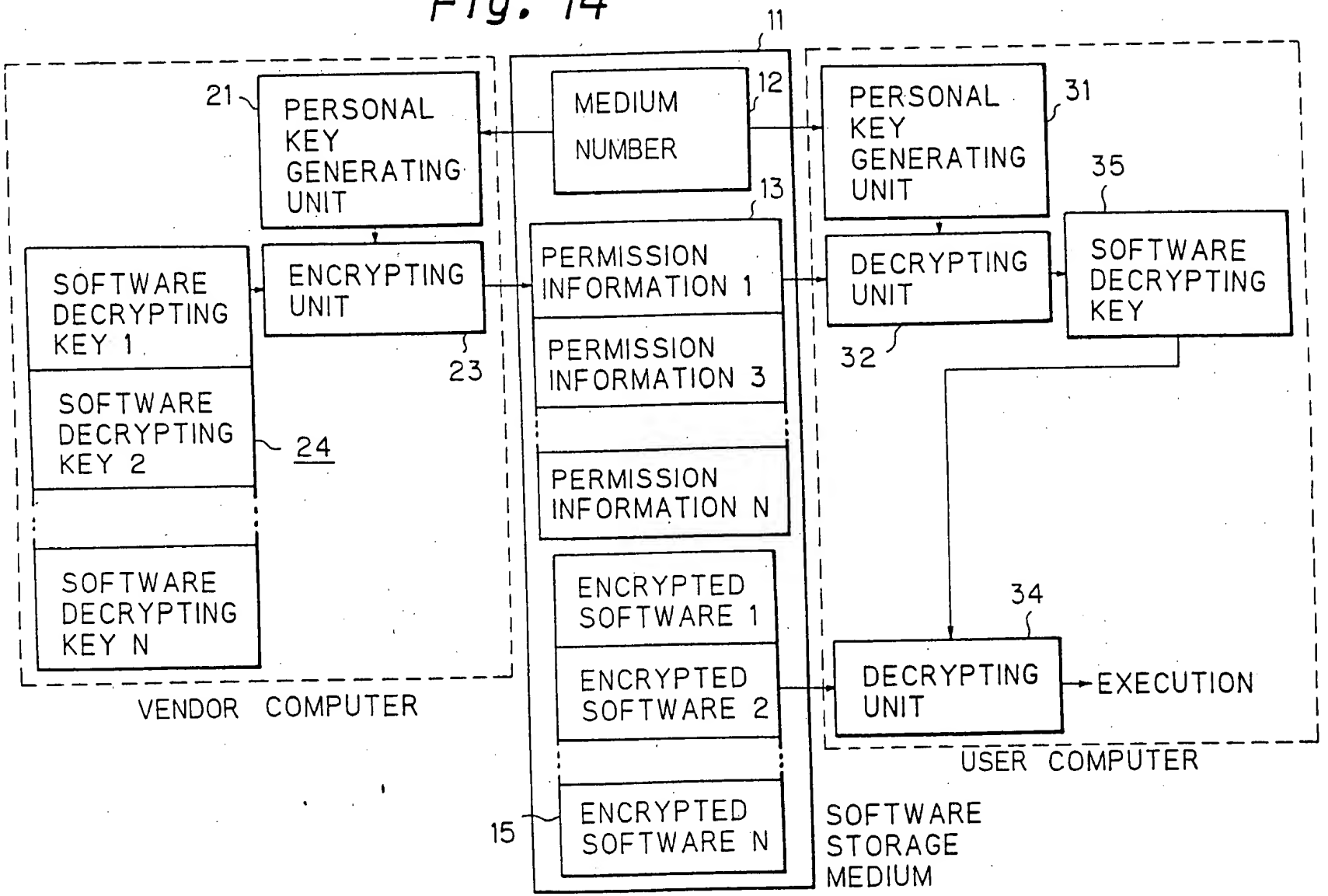

SOFTWARE STORAGE MEDIUM
11
MEDIUM NUMBER
12
ENCRYPTED SOFTWARE
15
PERMISSION INFORMATION
13
PERMISSION INFORMATION STRAGE MEDIUM
USER COMPUTER
PERSONAL KEY GENERATING UNIT
31
DECRYPTING UNIT
32
SOFTWARE DECRYPTING KEY
35
DECRYPTING UNIT
34
EXECUTION
VENDOR COMPUTER
PERSONAL KEY GENERATING UNIT
21
ENCRYPTING UNIT
23
SOFTWARE DECRYPTING KEY
24

Fig. 14


11
21
PERSONAL KEY GENERATING UNIT
MEDIUM NUMBER
12
PERSONAL KEY GENERATING UNIT
31
35
13
SOFTWARE DECRYPTING KEY 1
ENCRYPTING UNIT
PERMISSION INFORMATION 1
DECRYPTING UNIT
SOFTWARE DECRYPTING KEY
23
PERMISSION INFORMATION 3
32
SOFTWARE DECRYPTING KEY 2
24
PERMISSION INFORMATION N
ENCRYPTED SOFTWARE 1
34
SOFTWARE DECRYPTING KEY N
ENCRYPTED SOFTWARE 2
DECRYPTING UNIT
EXECUTION
VENDOR COMPUTER
USER COMPUTER
15
ENCRYPTED SOFTWARE N
SOFTWARE STORAGE MEDIUM

21/21